



**PCI-DSS Validation Guide for PCI ASSURE:
End to End Encryption (E2EE)**



PCI Simple Path to Compliance

PCI ASSURE is Global Payments Integrated easy to use solution for validating PCI compliance. PCI ASSURE eliminates complexity and allows merchants to address the most common security risks without excessive friction or overhead.

PCIASSURE®

A Service of  **openedge**
A division of **globalpayments**



PCI ASSURE – Here is What to Expect

- Global Payments Integrated offers a simplified path to compliance for eligible merchants using EMV devices capable of end-to-end encryption who are integrated with our Partners. This means merchants only answer 24 simple questions. The validation is good for the entire year and a reminder email is sent when it is time to re-validate.*
- PCI ASSURE provides access to Policy documents and Security awareness training for employees and management that meet the related requirements.
- Global Payments Integrated Compliance Services team is available for one-on-one guidance. If you have any questions you can use at complianceservices@openedgepay.com

**Note: This walkthrough document is meant to provide guidance for a typical merchant using Global Payments Integrated secure payment solutions. Merchants should evaluate their own payment environment to determine the presence of cardholder data related to this specific processing account, when answering not applicable for any individual requirement.*



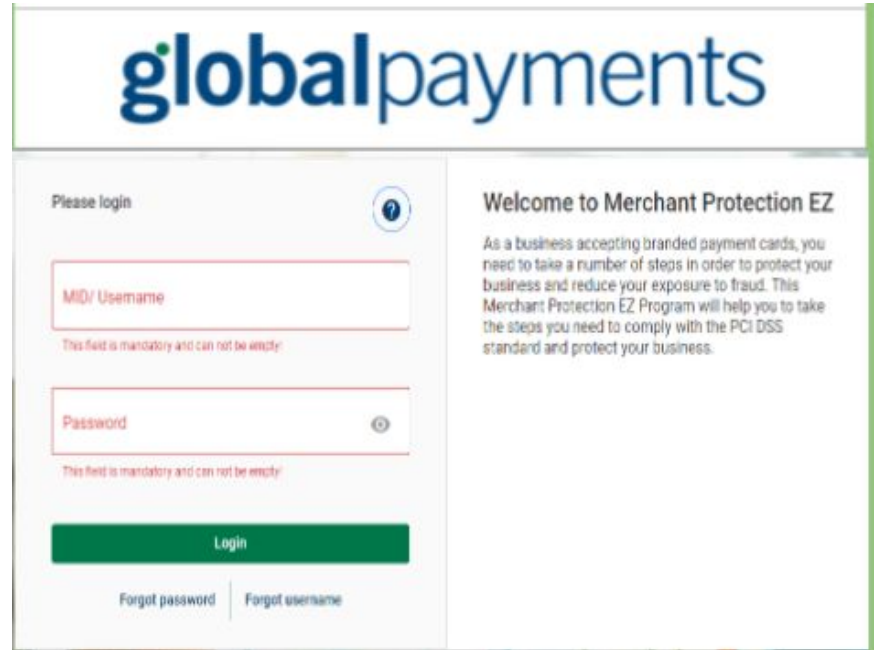
PCI ASSURE – How to Log in

- You will receive two emails from Sysnet within 30-45 days regarding our PCI ASSURE program.
- The first email will include your username and the second email will contain the temporary password.
- If you haven't received this email within that time frame, please contact us at complianceservices@openedgepay.com

PCI ASSURE – How to Log in

To access the PCI ASSURE portal for PCI validation, please follow the link in your welcome letter or the following url:

<https://www.pciassure.gpndi.com>



The screenshot shows the login interface for the Merchant Protection EZ program. At the top, the 'globalpayments' logo is displayed. Below the logo, the page is divided into two main sections. On the left, a 'Please login' section contains two input fields: 'MID/ Username' and 'Password'. Both fields have a red border and a red error message below them: 'This field is mandatory and can not be empty!'. The 'Password' field includes a toggle icon for visibility. Below the input fields is a green 'Login' button. At the bottom of this section are two links: 'Forgot password' and 'Forgot username'. On the right, a 'Welcome to Merchant Protection EZ' section contains a paragraph of text: 'As a business accepting branded payment cards, you need to take a number of steps in order to protect your business and reduce your exposure to fraud. This Merchant Protection EZ Program will help you to take the steps you need to comply with the PCI DSS standard and protect your business.'

PCI ASSURE – Using the Portal

Once on the Homepage you should see, “Welcome to Merchant Protection EZ” page

- From here, Enter “Your User/MID and Password”
- Then select “Login”

Please login ?

MID/ Username
This field is mandatory and can not be empty!

Password 👁
This field is mandatory and can not be empty!

Login

[Forgot password](#) | [Forgot username](#)

Welcome to Merchant Protection EZ

As a business accepting branded payment cards, you need to take a number of steps in order to protect your business and reduce your exposure to fraud. This Merchant Protection EZ Program will help you to take the steps you need to comply with the PCI DSS standard and protect your business.

PCI ASSURE – Using the Portal

- Once Logged in you should see the “What's Next?” landing page.
- From here, choose “Next “ or “Return to last Question” to begin questionnaire.

←

What's next?

- 1 We will ask you some questions
Mostly around how your business is set up to handle credit and debit card payments. Your answers help us to figure out the level of security risks that your business may have so we only ask you questions relevant to your business.
- 2 We will help you protect your business
To help you understand the areas of your business that might be at risk, you will be brought through your security assessment and any scanning if needs be.
- 3 Confirm your business is secure
You will be asked to confirm and validate your responses and any scanning tasks that you were required to undertake. PCI DSS refer to this as your Attestation of Compliance (AoC).

Getting Started
with PCI Data Security Standard

04:08

Return to last question



PCI ASSURE – The Self-Assessment Questionnaire

Let's walk a typical merchant through the self-assessment questionnaire as they validate PCI compliance.

- Once Logged in you should see the “Before you begin” page.
- From here, select “Next” to begin questionnaire.

Before you begin

Welcome to your new PCI DSS compliance portal. If we recently migrated you from the PCI DSS compliance portal, we have a streamlined process for you to complete your account profile, unless you have changed anything within your credit card processing environment.

Click next to proceed.



Previous

Next

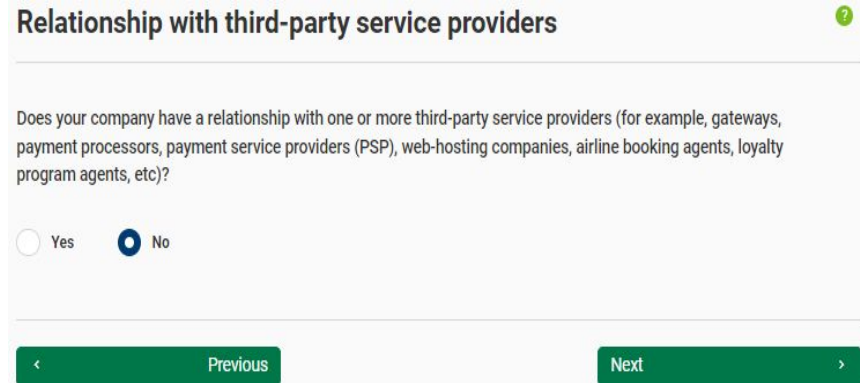


PCI ASSURE – The Self-Assessment Questionnaire

Global Payments Integrated is a Level 1 PCI-DSS validated Third Party Service Provider. PCI validation is listed [here](#)

You should see the “Relationship with third-party service providers” page.

- From here, select “No”
- Then Select “Next” to next question.



The screenshot shows a questionnaire interface with the following elements:

- Title:** Relationship with third-party service providers (with a green question mark icon in the top right corner).
- Question:** Does your company have a relationship with one or more third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc)?
- Options:** Two radio buttons are present: "Yes" (unselected) and "No" (selected).
- Navigation:** At the bottom, there are two green buttons: "Previous" (with a left arrow) and "Next" (with a right arrow).

PCI ASSURE – The Self-Assessment Questionnaire

This screen applies to the merchant and what their business would be classified as.

Using The “Filter” Bar you can search for what best applies to the merchant.

Start Complete

Select Your Merchant Type ?

Please use the selection tools below to describe the category and type of business that best describes your business. You can select multiple types.

Filter:

A/C, Refrigeration Repair Aquariums

- A/C, Refrigeration Repair
- Accounting/Bookkeeping Services
- Advertising Services
- Agricultural Cooperative
- Airlines
- Airlines Air Carriers

< Previous Next >

PCI ASSURE – The Self-Assessment Questionnaire

- Select “No” for this question.
- Click “Next” for the next question.

Start Complete

Payment Related Services ?

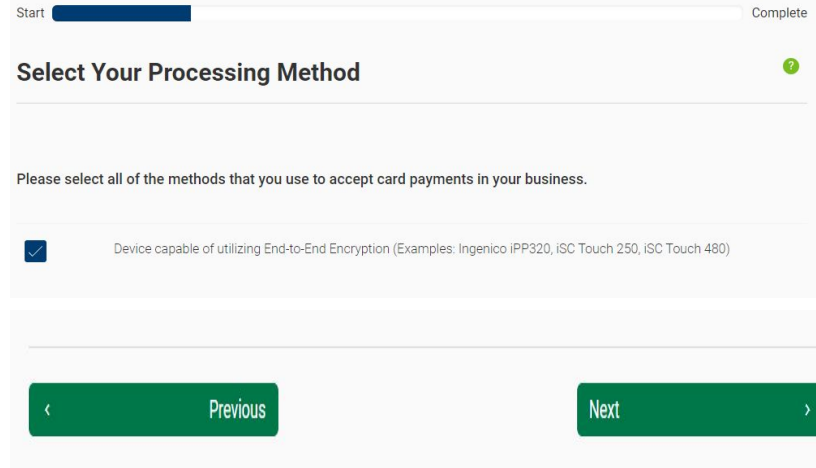
Does your organization handle credit card transactions in any manner other than payment acceptance for your goods and services? For example:

- Installing and Maintaining Credit Card Payment Devices for Other Organizations
- Taking Credit Card Transactions for Multiple Companies and Dispersing Payments To Those Businesses
- Selling Credit Card Payment Solutions

Yes No

< Previous Next >

PCI ASSURE – The Self-Assessment Questionnaire



The screenshot displays a progress bar at the top with 'Start' on the left and 'Complete' on the right. Below the progress bar is the title 'Select Your Processing Method' followed by a green question mark icon. The instruction reads: 'Please select all of the methods that you use to accept card payments in your business.' A single option is visible, which is checked: 'Device capable of utilizing End-to-End Encryption (Examples: Ingenico IPP320, iSC Touch 250, iSC Touch 480)'. At the bottom of the form are two green buttons: 'Previous' with a left arrow and 'Next' with a right arrow.

Select the first option for a secure POS using a device capable of utilizing End-to-End Encryption (Ingenico & Verifone EMV devices).*

**Note: Select the best Processing Method. Selecting multiple processing methods will result in a longer questionnaire. If you have questions about your processing method, please contact us at complianceservices@openedgepay.com*

PCI ASSURE – The Self-Assessment Questionnaire

- Choose “Yes” and choose next.

This qualifies for the shortened version of the SAQ-E2EE MERCH. After all the prerequisite questions are answered, you will be presented with 24 True or False questions.

To be validated PCI compliant within Sysnet, you will have to answer “True” or “Not-Applicable” to all 24.*

**Note: Answering “False” to any requirement will create a “to-do” list within PCI ASSURE which can be revisited once the requirement is met.*

The screenshot shows a progress bar at the top with 'Start' on the left and 'Complete' on the right. Below the progress bar is the section title 'Eligibility'. The main text reads: 'Please confirm the following: You have selected End-to-End Encryption (Example: iPP320, iSC250, iSC480) as your processing method. You will ONLY be presented with questions that apply to your selected processing method. All other questions will be PRE-ANSWERED as 'Not Applicable' and will not be presented to you.' Below this text is the question 'Do you agree with all of the above statements?' with two radio button options: 'Yes' (which is selected) and 'No'. At the bottom of the form are two green buttons: 'Previous' with a left arrow and 'Next' with a right arrow.

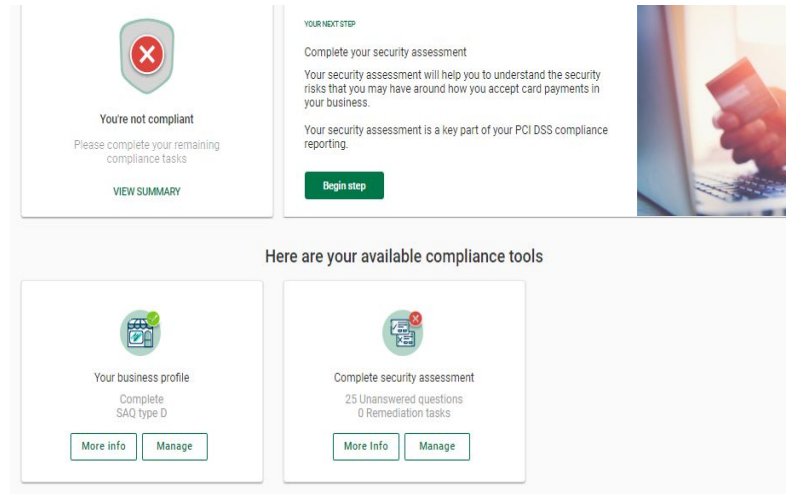
PCI ASSURE – Home / Main Screen

Your screen you will go to your home page and you will see these.

- Select “Begin Step”

Or:

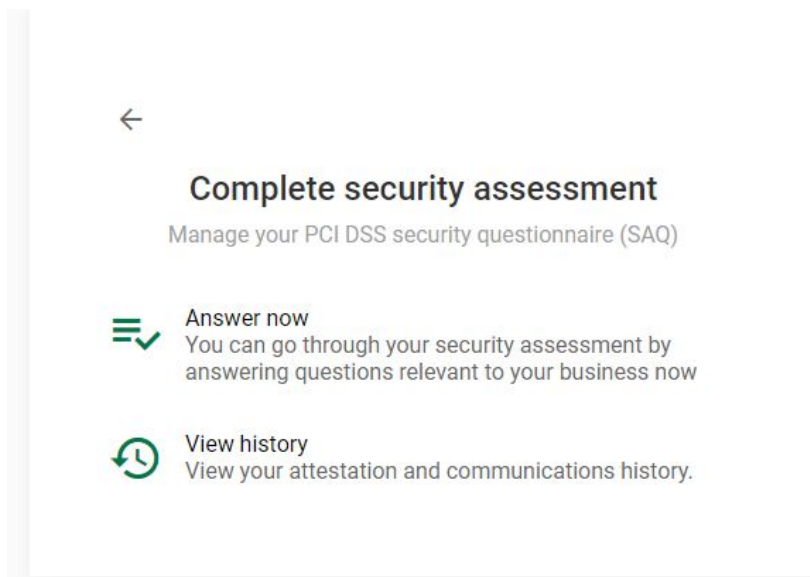
- Your next task will be to look for “Complete Activity Assessment”
- Then select “Manage” button



The screenshot displays the PCI ASSURE Home / Main Screen. At the top left, there is a shield icon with a red 'X' inside, indicating non-compliance. Below this icon, the text reads "You're not compliant" and "Please complete your remaining compliance tasks". A "VIEW SUMMARY" button is located below the text. To the right of this section, there is a "YOUR NEXT STEP" section with the heading "Complete your security assessment". Below this heading, there is a paragraph of text: "Your security assessment will help you to understand the security risks that you may have around how you accept card payments in your business." and another paragraph: "Your security assessment is a key part of your PCI DSS compliance reporting." A green "Begin step" button is positioned below the text. To the right of the "Begin step" button, there is a small image of a hand holding a credit card over a laptop. Below these sections, there is a heading "Here are your available compliance tools". Under this heading, there are two cards. The first card is titled "Your business profile" and shows a calendar icon with a green checkmark. Below the title, it says "Complete SAQ type D". There are two buttons: "More info" and "Manage". The second card is titled "Complete security assessment" and shows a shield icon with a red 'X' and a document icon. Below the title, it says "25 Unanswered questions" and "0 Remediation tasks". There are two buttons: "More Info" and "Manage".

PCI ASSURE – The Self-Assessment Questionnaire

Once on this page select “Answer Now” to start the questionnaire.



PCI – The Self-Assessment Questionnaire

- Protect Cardholder Data Section

Each section has questions that should be answered as “YES or N/A” in order to be considered compliant. Choosing “No” will create a “to do” list for reference.

First Question Part 2:

Answering the following question 3.1(a)

Ensuring that your network does not keep cardholder data and properly disposes of the sensitive information when cardholder data is no longer needed to be stored. Select “Yes or N/A”, the next question will come up automatically.


The screenshot displays the 'Protect Cardholder Data' section of the PCI Self-Assessment Questionnaire. At the top, there are filters for 'Show me: Only unanswered questions' and 'Show Help Text:'. A note below reads: 'Please note, some answered questions may remain shown in order to provide appropriate context status'. The main heading is 'Protect Cardholder Data' with the sub-heading 'Protect stored cardholder data'. The question text is: 'Are data-retention and disposal policies, procedures, and processes implemented as follows: 3.1(a) Is data storage amount and retention time limited to that required for legal, regulatory, and/or business requirements?'. Below the question, there is a green link: 'I have implemented a compensating control'. At the bottom, there are three buttons: 'N/A' (green), 'No' (red), and 'Yes' (green). On the right side, there is a sidebar with 'Sections' and 'Milestones' tabs. The 'Milestones' tab is active, showing a list of 11 items with status indicators: 1. Build and Maintain a Secure Network and Systems (green checkmark), 2. Protect Cardholder Data (5 in a circle), 3. Maintain a Vulnerability Management Program (green checkmark), 4. Implement Strong Access Control Measures (8 in a circle), 5. Regularly Monitor and Test Networks (1 in a circle), 6. Maintain an Information Security Policy (11 in a circle), and 7. Confirm your compliance (red X).

PCI – The Self-Assessment Questionnaire

- Protect Cardholder Data Section


Protect Cardholder Data
Protect stored cardholder data


Are data-retention and disposal policies, procedures, and processes implemented as follows:

3.1(d) 








Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?

I have implemented a compensating control

 **Compliance maintenance task**
To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last completion date:
 

Sections **Milestones**

-  Build and Maintain a Secure Network and Systems
-  Protect Cardholder Data
-  Maintain a Vulnerability Management Program
-  Implement Strong Access Control Measures
-  Regularly Monitor and Test Networks
-  Maintain an Information Security Policy
-  Confirm your compliance

Answering the following question 3.1(d)

- Choose “Yes or N/A”
- Select Compliance Maintenance date they performed. “Calendar / Enter date” and choose “finish”

Merchants are responsible to ensure that there is no cardholder data present in their networks. PAN discovery tools can confirm that cardholder data is not leaking out of the payment solution and/or being introduced to the system through other means (email, incorrect data entry, etc.)

PCI – The Self-Assessment Questionnaire

- Protect Cardholder Data Section

Protect Cardholder Data

Protect stored cardholder data

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

3.2.2

The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?

I have implemented a compensating control

N/A

No

Yes

Sections

Milestones

- ✓ Build and Maintain a Secure Network and Systems
- ③ Protect Cardholder Data
- ✓ Maintain a Vulnerability Management Program
- ⑧ Implement Strong Access Control Measures
- ① Regularly Monitor and Test Networks
- ⑪ Maintain an Information Security Policy
- ✗ Confirm your compliance

Part 2:

Answering the following question 3.2.2

- Choose “Yes or N/A”

Verifying that you do not store CVV (3 digit code) from card and its securely deleted after transaction has taken place. Our secure payment solutions do not store this data.

PCI – The Self-Assessment Questionnaire

Protect Cardholder Data Section

3.3 ✓

Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN?

Note: This requirement does not supersede stricter requirements in place for displays of cardholder data for example, legal or payment card brand requirements for point-of-sale (POS) receipts.

I have implemented a compensating control

N/A

No

Yes

Part 2:

Answering the following question 3.3

- Select “Yes or N/A” for next question

Confirm that primary account number Primary Account Number (PAN) First 6 digits and last 4 digits to be displayed) is correctly masked.

PCI – The Self-Assessment Questionnaire

– Protect Cardholder Data Section

3.7 

Are security policies and operational procedures for protecting stored cardholder data:

- Documented
- In use
- Known to all affected parties?

I have implemented a compensating control

N/A

No

Yes

Answering the following question
3.7

- Select “Yes or N/A” for next question

Examine Documents, apps, and all parties that have an affect on procedures of protecting cardholder data.

PCI – The Self-Assessment Questionnaire

- Protect Cardholder Data Section

Show me: Show Help Text:

Please note, some answered questions may remain shown in order to provide appropriate context status

Protect Cardholder Data

i There are no unanswered questions in this section

Attention! You may still have questions answered "No", which means that your security assessment will not be complete until you address compliance remediation tasks associated with those questions you have answered "No"


< Previous Next >

Finished Section 2 of answering questions.

Select "Next", the next section will display and will continue asking questions.

PCI – The Self-Assessment Questionnaire

- Implement Strong Access Control Measures

9.5 

Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?
For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.

I have implemented a compensating control

N/A No Yes

Answering the following question 9.5

- Select “Yes or N/A” for next question

If the merchant stores credit card numbers on paper forms they must be securely stored and properly disposed. This technically also applies to hard drives and other electronic media which also need to be destroyed when no longer in use.

PCI – The Self-Assessment Questionnaire

- Implement Strong Access Control Measures

9.8(a) ✓

Is all media destroyed when it is no longer needed for business or legal reasons?

I have implemented a compensating control

N/A

No

Yes

Part 2:

Answering the following question
9.8(a)

- Choose “Yes or N/A” for next question

Dispose of hard copies and or virtual instances of cardholder data properly and when it is no longer needed.

PCI – The Self-Assessment Questionnaire

- Implement Strong Access Control Measures

9.8(b) ✓

Is there a periodic media destruction policy that defines requirements for the following?

- Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
- Storage containers used for materials that are to be destroyed must be secured.
- Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).

I have implemented a compensating control

N/A

No

Yes

Is media destruction performed as follows:

Part 2:

Answering the following question
9.8(b)

- Select “Yes or N/A” for next question

This is explaining how to properly store and dispose of sensitive information.

PCI – The Self-Assessment Questionnaire

- Implement Strong Access Control Measures

9.9.1(a) ✓

Does the list of devices include the following?

- Make, model of device
- Location of device (for example, the address of the site or facility where the device is located)
- Device serial number or other method of unique identification

I have implemented a compensating control

N/A

No

Yes

Part 2:

Answering the following question
9.9.1(a)


- Select “Yes or N/A” for next question

Merchants must keep track of the location and and serial number of point of interaction (swipe) devices in order to make sure they are not swapped out.

PCI – The Self-Assessment Questionnaire

- Implement Strong Access Control Measures

Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?

9.9.3(a) 

Do training materials for personnel at point-of-sale locations include the following?

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

I have implemented a compensating control

N/A

No

Yes

Part 2:

Answering the following question
9.9.3(a)

- Select “Yes or N/A” for next question

Merchants must train personnel to ensure that devices are not swapped, tampered with or substituted.

PCI – The Self-Assessment Questionnaire

– Implement Strong Access Control Measures

Show me: Show Help Text:

Please note, some answered questions may remain shown in order to provide appropriate context status

Implement Strong Access Control Measures

i There are no unanswered questions in this section
Attention! You may still have questions answered "No", which means that your security assessment will not be complete until you address compliance remediation tasks associated with those questions you have answered "No"

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

Sections **Milestones**

- ✓ Build and Maintain a Secure Network and Systems
- ⑤ Protect Cardholder Data
- ✓ Maintain a Vulnerability Management Program
- ⑧ Implement Strong Access Control Measures
- ① Regularly Monitor and Test Networks
- ⑩ Maintain an Information Security Policy
- ✗ Confirm your compliance

Finished Section 2 of answering questions.

Select "Next", the next section will display and will continue asking questions.

PCI – The Self-Assessment Questionnaire

- Regularly Monitor & Test Networks

Is time data protected as follows:

10.4.2(a) ✓

Is access to time data restricted to only personnel with a business need to access time data?

I have implemented a compensating control

N/A

No

Yes

Part 3:

Answering the following question
10.4.2(a)

- Select “Yes or N/A” for next question

If a merchant has a dedicated central time server it can only be accessed by personnel with a business need.

PCI – The Self-Assessment Questionnaire

- Regularly Monitor & Test Networks

SHOW ME: SHOW HELP TEXT:

Please note, some answered questions may remain shown in order to provide appropriate context status

Regularly Monitor and Test Networks

i There are no unanswered questions in this section

Attention! You may still have questions answered "No", which means that your security assessment will not be complete until you address compliance remediation tasks associated with those questions you have answered "No"

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

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy
- Confirm your compliance

Finished Section 4 of answering questions.

Select "Next", the next section will display and will continue asking questions.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

12.1 ✓

Is a security policy established, published, maintained, and disseminated to all relevant personnel?

I have implemented a compensating control

N/A No Yes

Part 5:

Answering the following question 12.1

- Choose “Yes or N/A” for next question.

All merchants should have a security policy document or include relevant security policies and procedures within their employee handbook.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

12.1.1 ✓

Is the security policy reviewed at least annually and updated when the environment changes?

I have implemented a compensating control

N/A No Yes

Part 5:

Answering the following question
12.1.1

- Choose “Yes or N/A” for next question.

Merchants should review the security policy annually to ensure that any changes to security policies and procedures are documented.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

12.4 ✓

Do security policy and procedures clearly define information security responsibilities for all personnel?

I have implemented a compensating control

N/A

No

Yes

Part 5:

Answering the following question 12.4

- Choose “Yes or N/A” for next question.

Policy documents should indicate which roles are responsible for managing compliance with specific requirements.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

12.5(a) ✓

Is responsibility for information security formally assigned to a Chief Security Officer or other security-knowledgeable member of management?

Are the following information security management responsibilities formally assigned to an individual or team:

I have implemented a compensating control

N/A

No

Yes

Part 5:

Answering the following question 12.5(a)

- Choose “Yes or N/A” for next question.

Formal assignment of overall information security must be part of security policy and procedure documentation.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

12.6(a) ✓

Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?

Do security awareness program procedures include the following:

I have implemented a compensating control

N/A

No

Yes

Part 5:

Answering the following question 12.6(a)

- Choose “Yes or N/A” for next question.

Merchants must have an annual security training program in place to ensure employees are aware of policies and procedures.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

12.8.1 

Is a list of service providers maintained, including a description of the service(s) provided?

I have implemented a compensating control

N/A

No

Yes

Part 5:

Answering the following question
12.8.1

- Choose “Yes or N/A” for next question.

Merchants must be aware of all service providers who could affect the security of their customers cardholder data.

PCI – The Self-Assessment Questionnaire

Maintain an Information Security Policy

12.8.2 ✓

Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?

Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.

I have implemented a compensating control

N/A

No

Yes

Part 5 :

Answering the following question
12.8.2

- Choose “Yes or N/A” for next question.

Merchants sign a written merchant agreement when boarding with Global Payments Integrated.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

12.8.3 ✓

Is there an established process for engaging service providers, including proper due diligence prior to engagement?

I have implemented a compensating control

N/A

No

Yes

Part 5:

Answering the following question
12.8.3

- Choose “Yes or N/A” for next question.

Merchants should confirm that service providers are PCI compliant and/or include the third party services as part of their validation. Global Payments Integrated is a PCI DSS Level 1 Validated service provider.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

12.8.4 ✓

Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?

N/A

No

Yes

Part 5:

Answering the following question
12.8.4

- Choose “Yes or N/A” for next question.

Merchants should check the PCI compliance status of service providers annually.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

12.8.5 ✓

Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?

N/A

No

Yes

Part 5:

Answering the following question 12.8.5

- Choose “Yes or N/A” for next question.

Global Payments Integrated does not typically require merchants to submit a “responsibility matrix”. Merchants should be aware that they are ultimately responsible for compliance with applicable PCI DSS requirements.

PCI – The Self-Assessment Questionnaire

- Maintain an Information Security Policy

Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:

12.10.1(a) ✓

Has an incident response plan been created to be implemented in the event of system breach?

I have implemented a compensating control

N/A

No

Yes

Part 5:

Answering the following question
12.10.1(a)

- Choose “Yes or N/A” for next question.

Merchants must have a plan to respond to a suspected compromise. The plan must include notification of the payment brands, business continuity plan, and data backup plan..

PCI – The Self-Assessment Questionnaire - Maintain an Information Security Policy

Show me: Show Help Text:

Please note, some answered questions may remain shown in order to provide appropriate context status

Maintain an Information Security Policy

i There are no unanswered questions in this section

Attention! You may still have questions answered "No", which means that your security assessment will not be complete until you address compliance remediation tasks associated with those questions you have answered "No"

[< Previous](#) [Next >](#)

Finished Section 5 of answering questions.

Select "Next", the next section will display and will continue asking questions.

PCI – The Self-Assessment Questionnaire

- Confirm you Compliance

- Choose “Confirm Your Attestation” to exit questionnaire.

It will take you back to Main screen.

It will also show that you are PCI compliant.

Confirm your compliance

Please review the form below and ensure all sections are correct and complete.

✓ Your organization information details

Company name GPI Test Merchant 2 - Csimmoms	Contact name Caitlin Simmons
Title	Telephone numbers
Email address csimmoms@tsys.com	Business address
Country USA	

✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ C1_VT

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

✓ Attestation



Information for Submission.

Based on the results noted in the SAQ C-VT dated Apr 6, 2022, the signatories identified in Parts 1.1, assert(s) the following compliance status for the entity identified in Part 2 of this document as of Apr 6, 2022:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby GPI Test Merchant 2 - Csimmoms has demonstrated full compliance with the PCI DSS.

Confirm your Attestation

Previous

Sections

- ✓ Build and Maintain a Secure Network and Systems
- ✓ Protect Cardholder Data
- ✓ Maintain a Vulnerability Management Program
- ✓ Implement Strong Access Control Measures
- ✓ Regularly Monitor and Test Networks
- ✓ Maintain an Information Security Policy
- ✓ Confirm your compliance