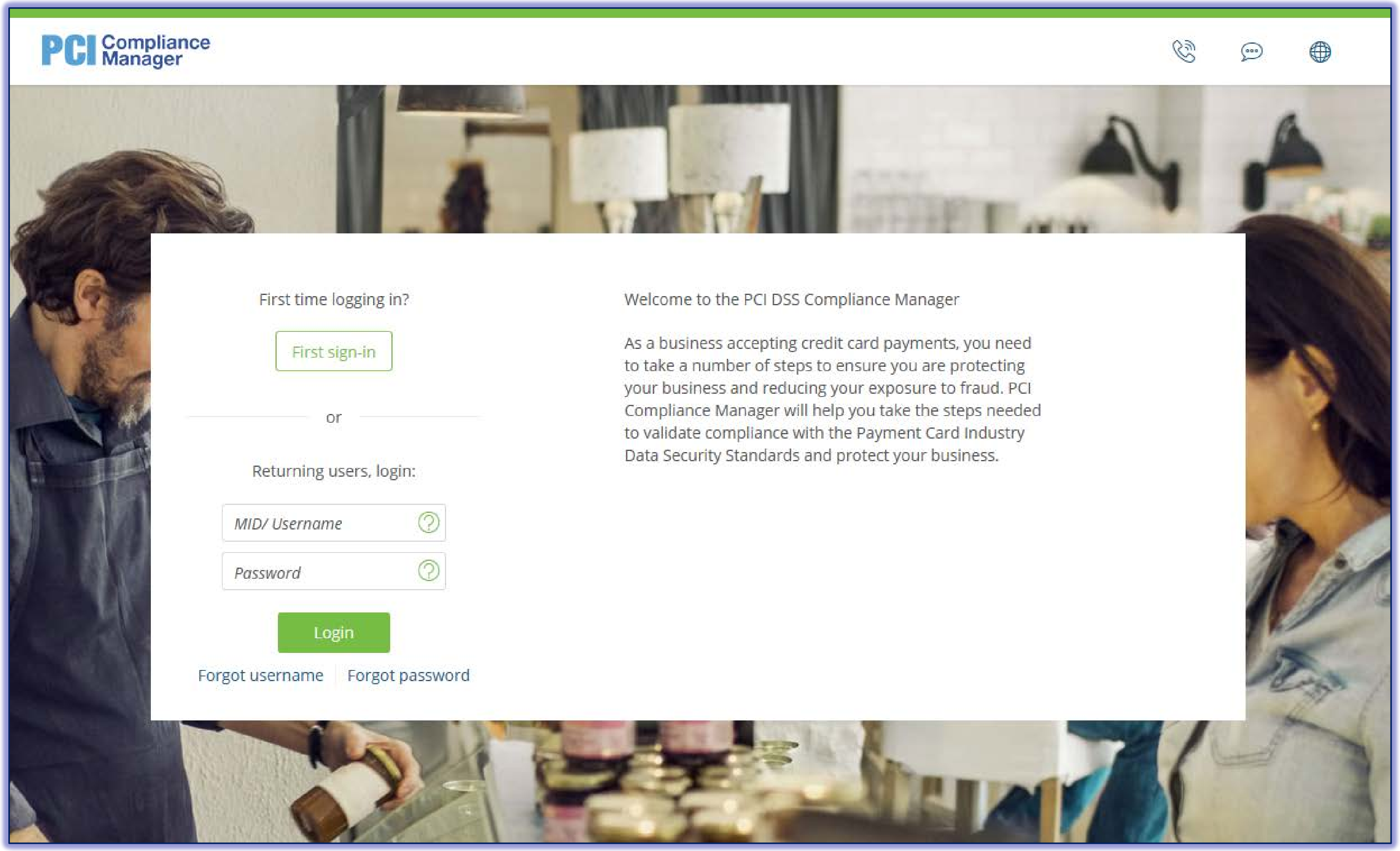
PCI Compliance Manager Demo

Elavon

Powering payments to grow your business / Powering payments to grow your business / Power

Getting Started

PCI Compliance Manager



First time logging in?

First sign-in

or

Returning users, login:

MID/ Username

Password

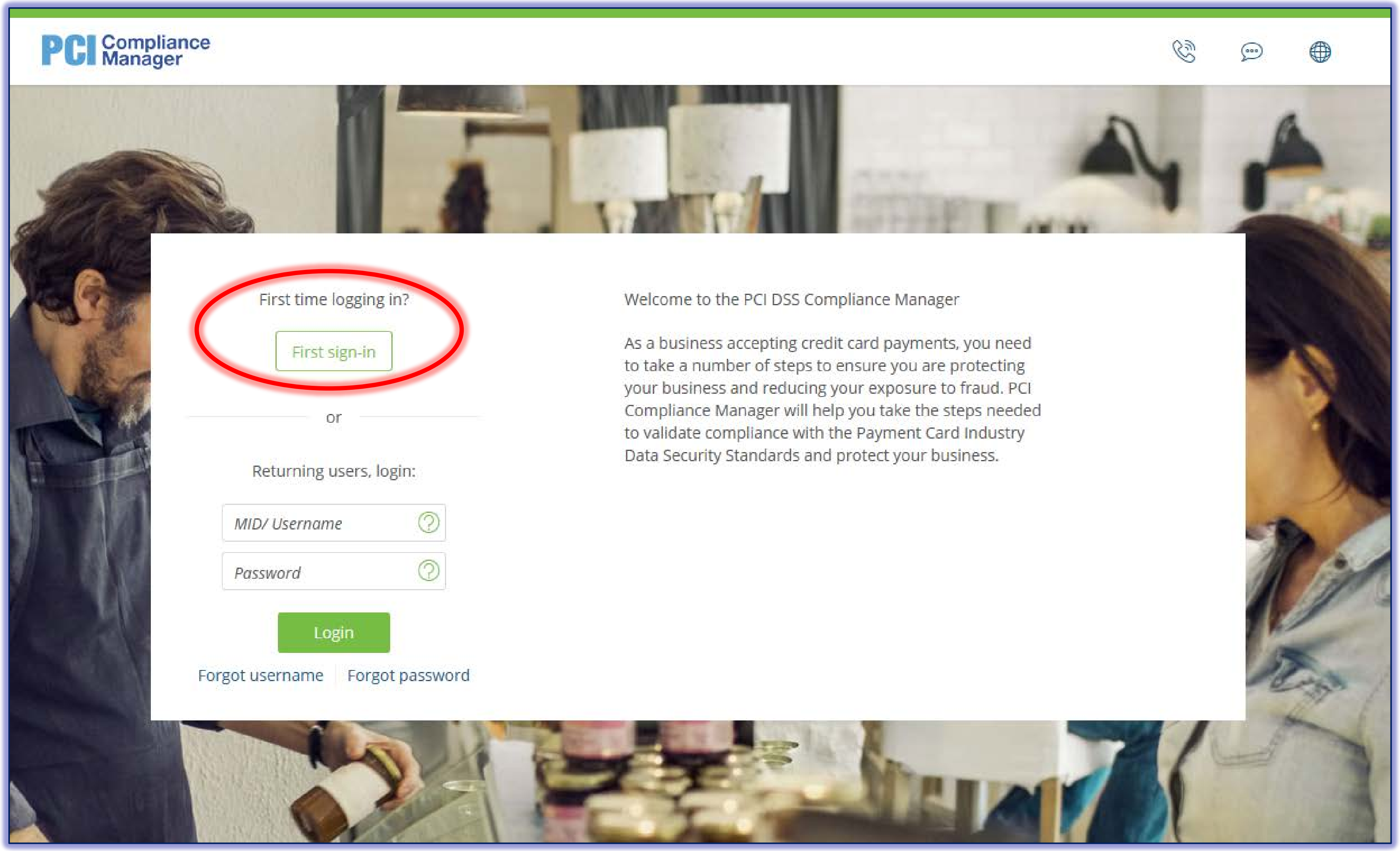
Login

Forgot username | Forgot password

Welcome to the PCI DSS Compliance Manager

As a business accepting credit card payments, you need to take a number of steps to ensure you are protecting your business and reducing your exposure to fraud. PCI Compliance Manager will help you take the steps needed to validate compliance with the Payment Card Industry Data Security Standards and protect your business.

Getting Started



First time logging in?

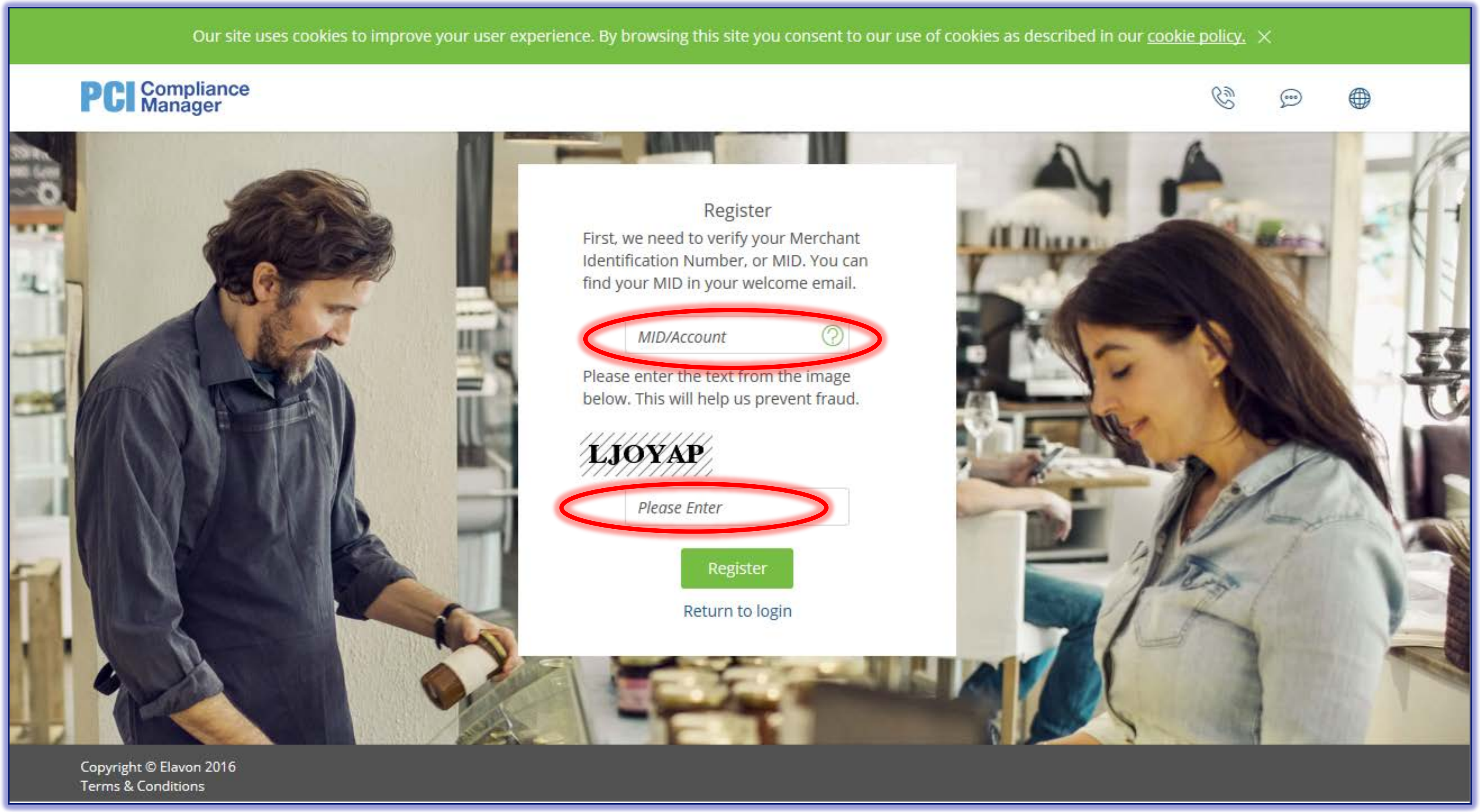
or

Returning users, login:

Welcome to the PCI DSS Compliance Manager

As a business accepting credit card payments, you need to take a number of steps to ensure you are protecting your business and reducing your exposure to fraud. PCI Compliance Manager will help you take the steps needed to validate compliance with the Payment Card Industry Data Security Standards and protect your business.

Getting Started



Our site uses cookies to improve your user experience. By browsing this site you consent to our use of cookies as described in our cookie policy.

PCI Compliance Manager

Register

First, we need to verify your Merchant Identification Number, or MID. You can find your MID in your welcome email.

MID/Account

Please enter the text from the image below. This will help us prevent fraud.

LJOYAP

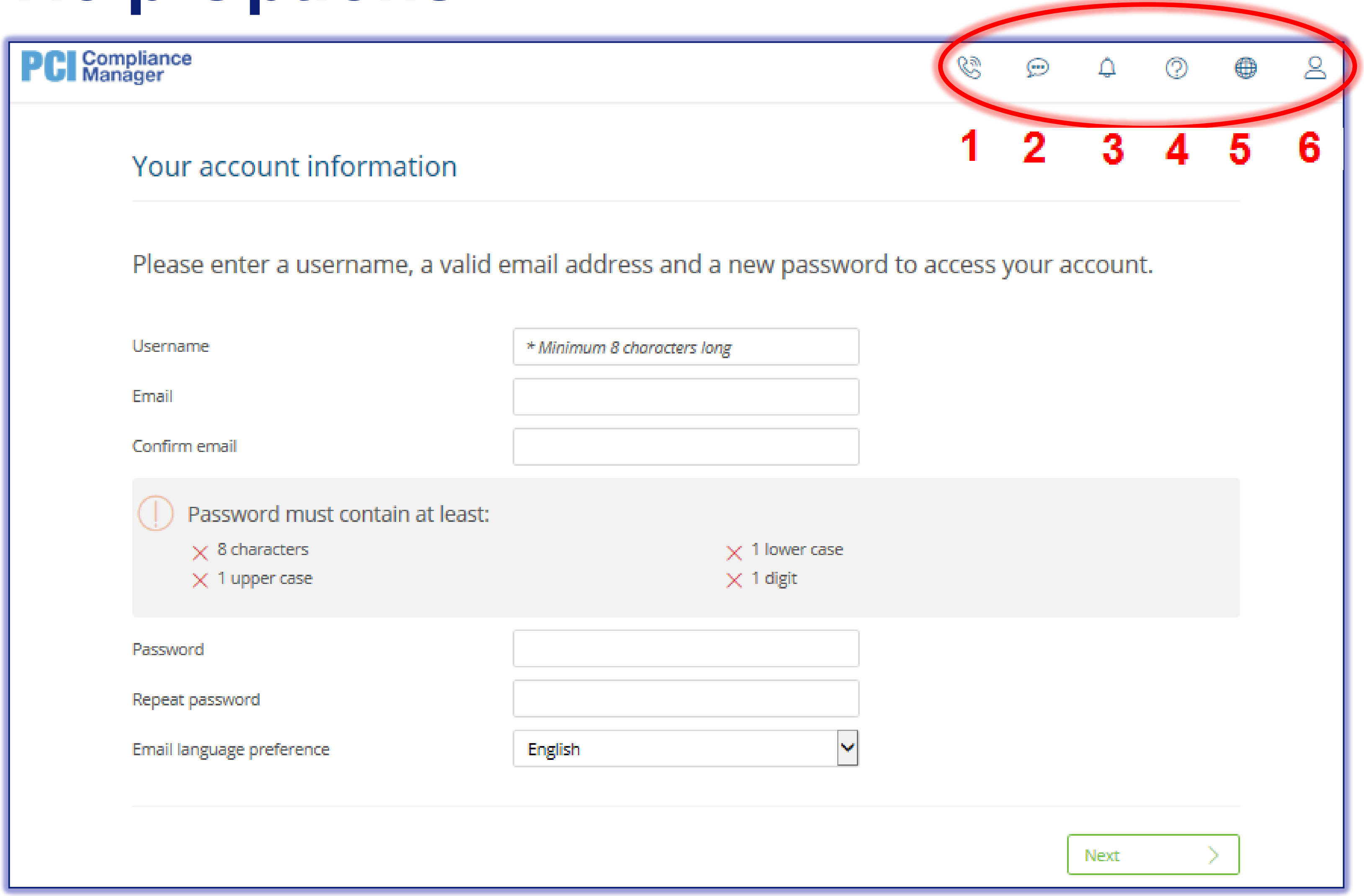
Please Enter

Register

Return to login

Copyright © Elavon 2016
Terms & Conditions

Help Options



Your account information

Please enter a username, a valid email address and a new password to access your account.

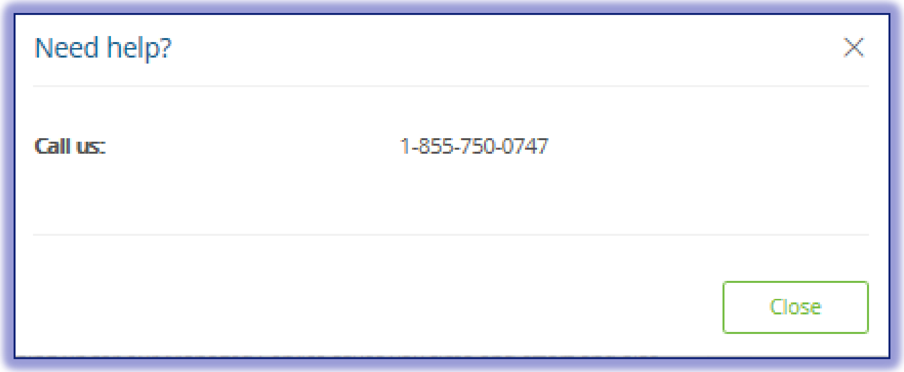
Username	* Minimum 8 characters long
Email	
Confirm email	

Password must contain at least:

- ✗ 8 characters
- ✗ 1 upper case
- ✗ 1 lower case
- ✗ 1 digit

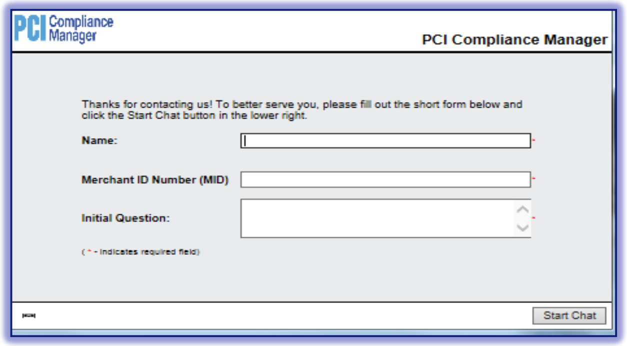
Password	
Repeat password	
Email language preference	English

Closer Look



Need help?

Call us: 1-855-750-0747



PCI Compliance Manager

Thanks for contacting us! To better serve you, please fill out the short form below and click the Start Chat button in the lower right.

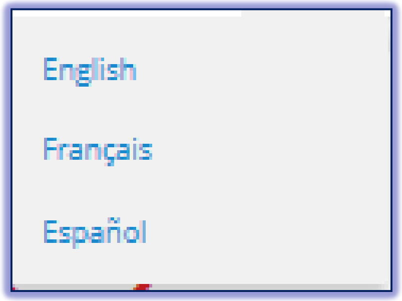
Name:

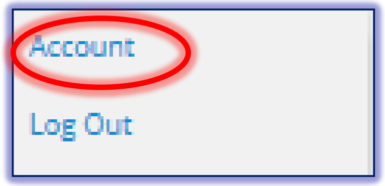
Merchant ID Number (MID)

Initial Question:

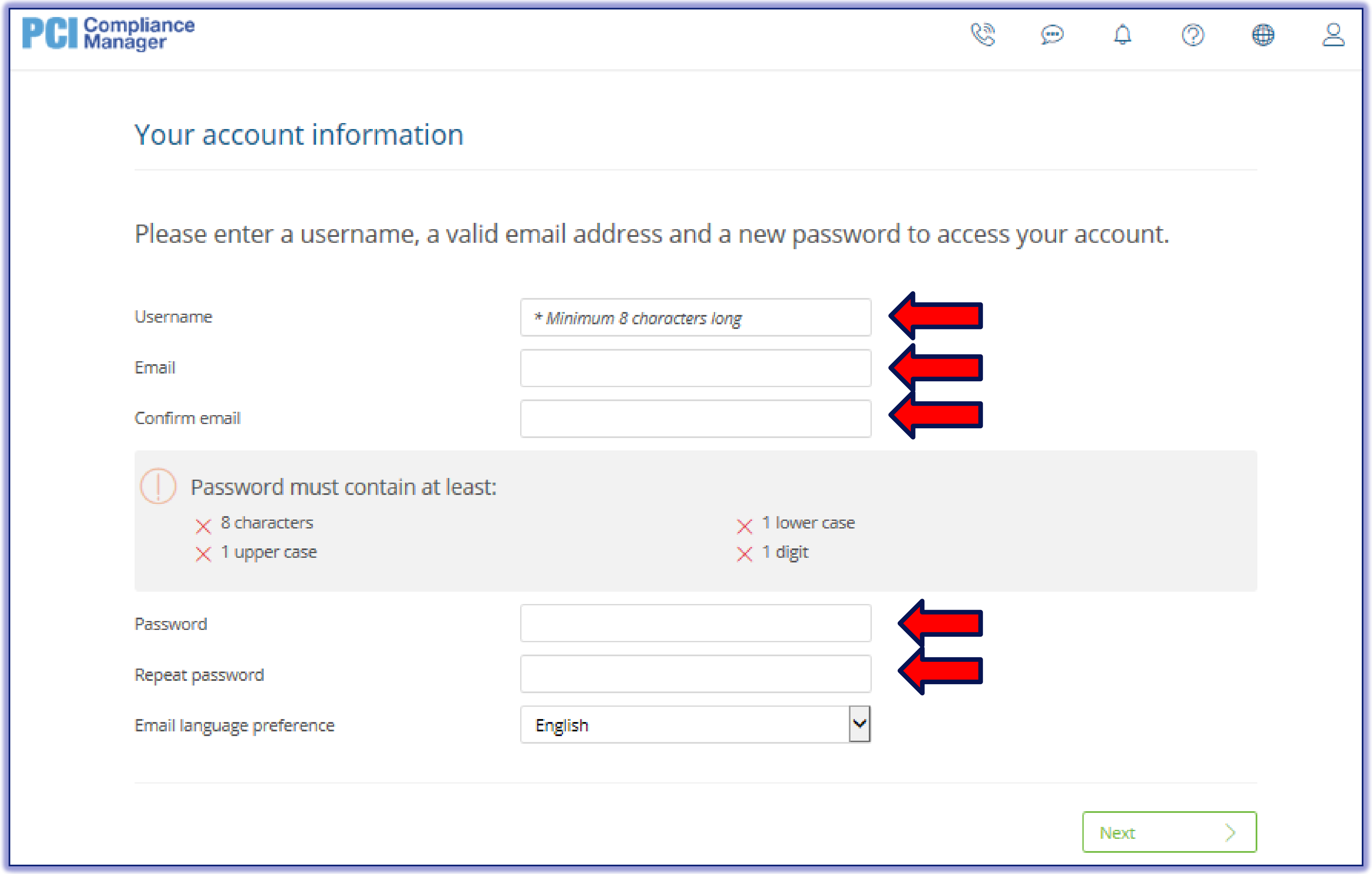
(* - Indicates required field)

You have no new notifications





Registration



Your account information

Please enter a username, a valid email address and a new password to access your account.

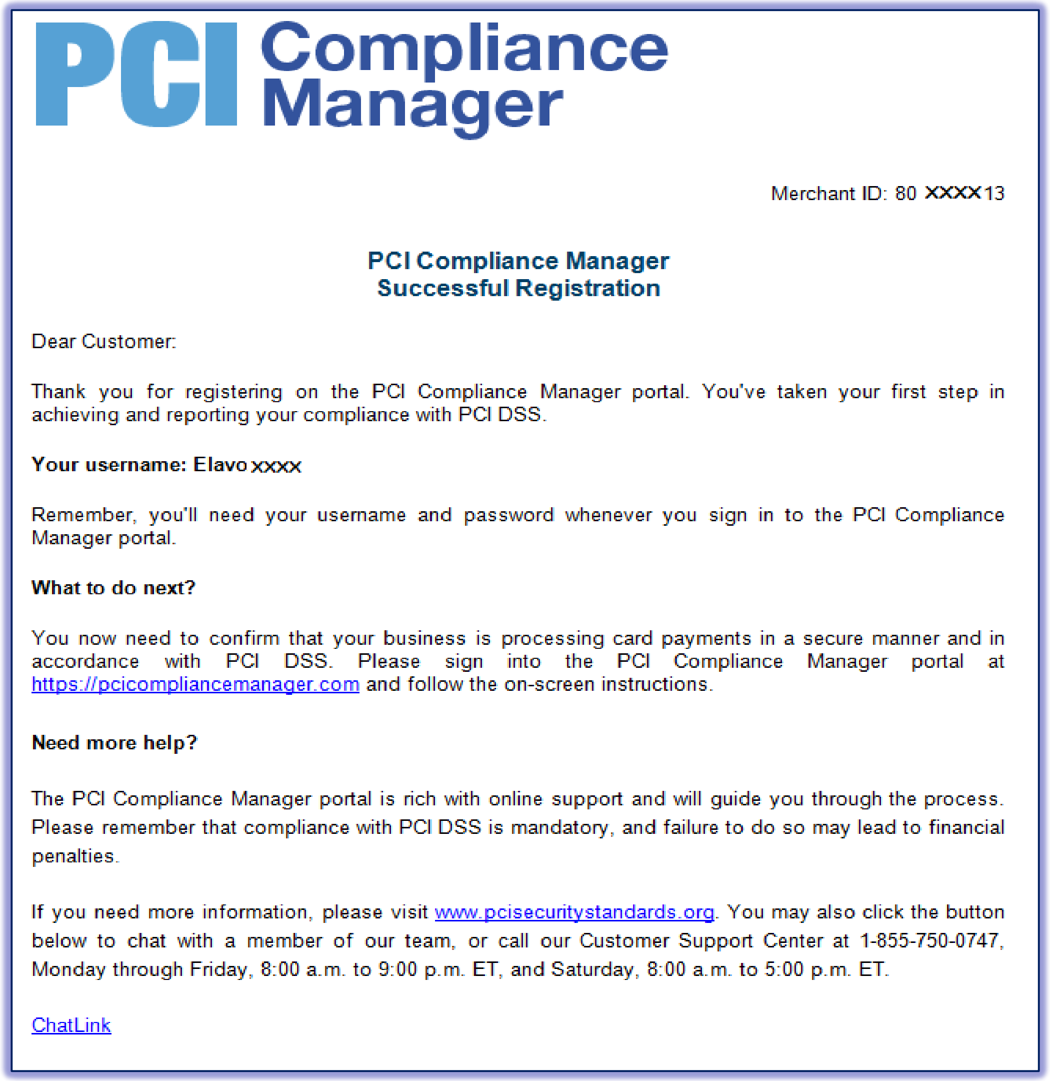
Username	* Minimum 8 characters long
Email	
Confirm email	

Password must contain at least:

- ✗ 8 characters
- ✗ 1 upper case
- ✗ 1 lower case
- ✗ 1 digit

Password	
Repeat password	
Email language preference	English

Welcome E-mail



PCI Compliance Manager

Merchant ID: 80 XXXX13

PCI Compliance Manager
Successful Registration

Dear Customer:

Thank you for registering on the PCI Compliance Manager portal. You've taken your first step in achieving and reporting your compliance with PCI DSS.

Your username: Elavo xxxx

Remember, you'll need your username and password whenever you sign in to the PCI Compliance Manager portal.

What to do next?

You now need to confirm that your business is processing card payments in a secure manner and in accordance with PCI DSS. Please sign into the PCI Compliance Manager portal at https://pcicompliancemanager.com and follow the on-screen instructions.

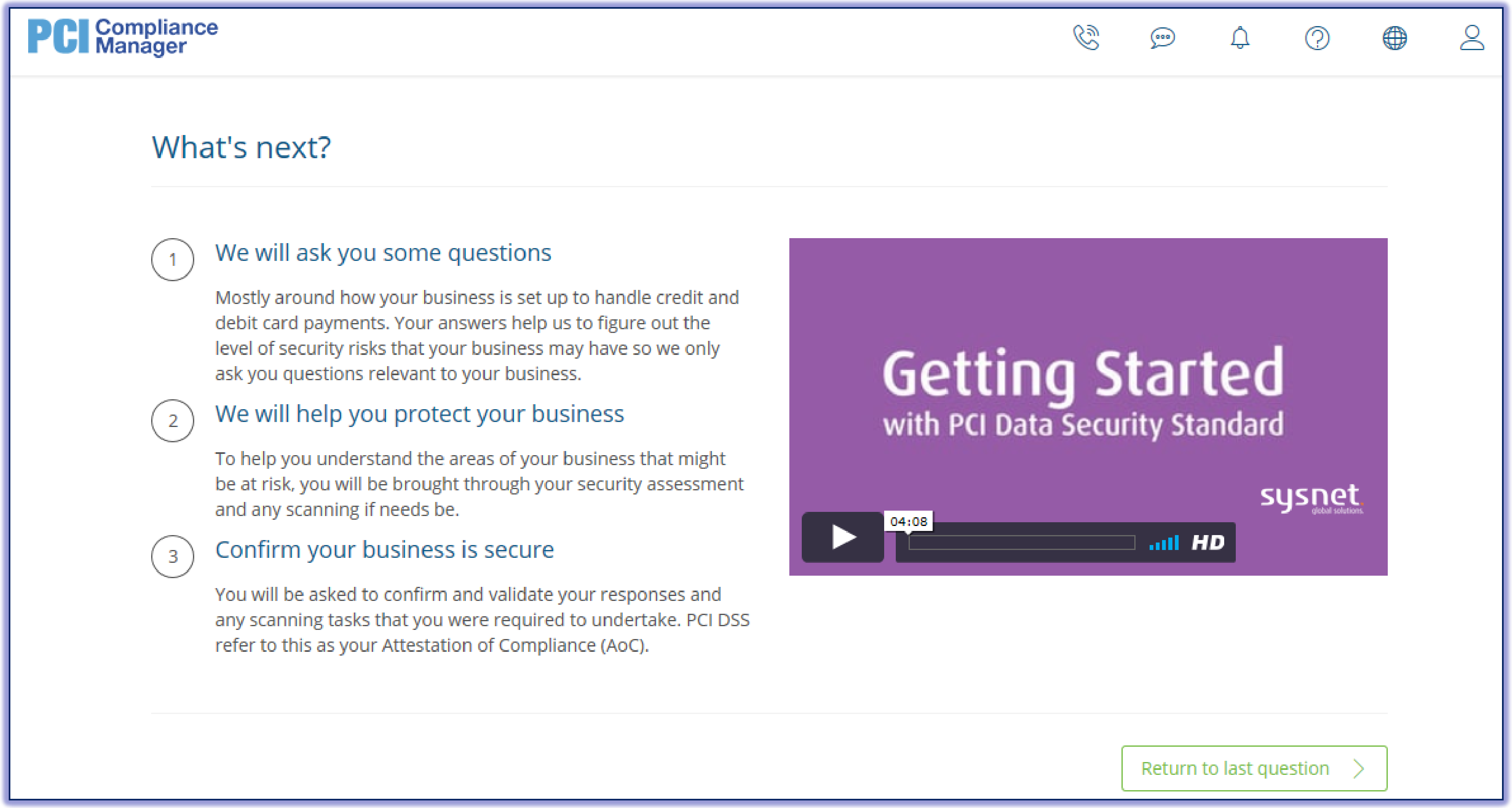
Need more help?

The PCI Compliance Manager portal is rich with online support and will guide you through the process. Please remember that compliance with PCI DSS is mandatory, and failure to do so may lead to financial penalties.

If you need more information, please visit www.pcisecuritystandards.org. You may also click the button below to chat with a member of our team, or call our Customer Support Center at 1-855-750-0747, Monday through Friday, 8:00 a.m. to 9:00 p.m. ET, and Saturday, 8:00 a.m. to 5:00 p.m. ET.

ChatLink

Getting Started



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

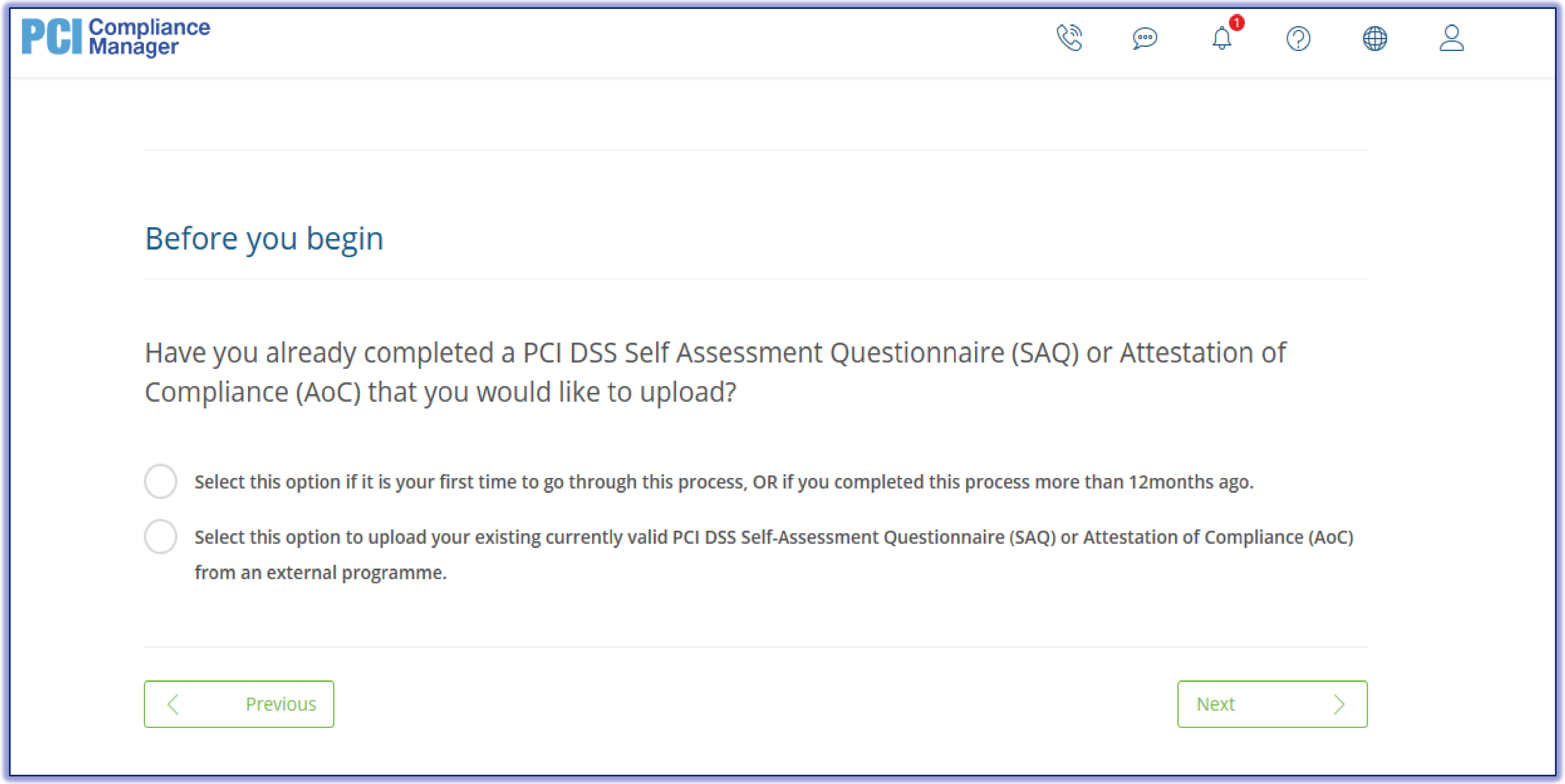
To help you understand the areas of your business that might be at risk, you will be brought through your security assessment and any scanning if needs be.

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).

Profile

Validation Confirmation



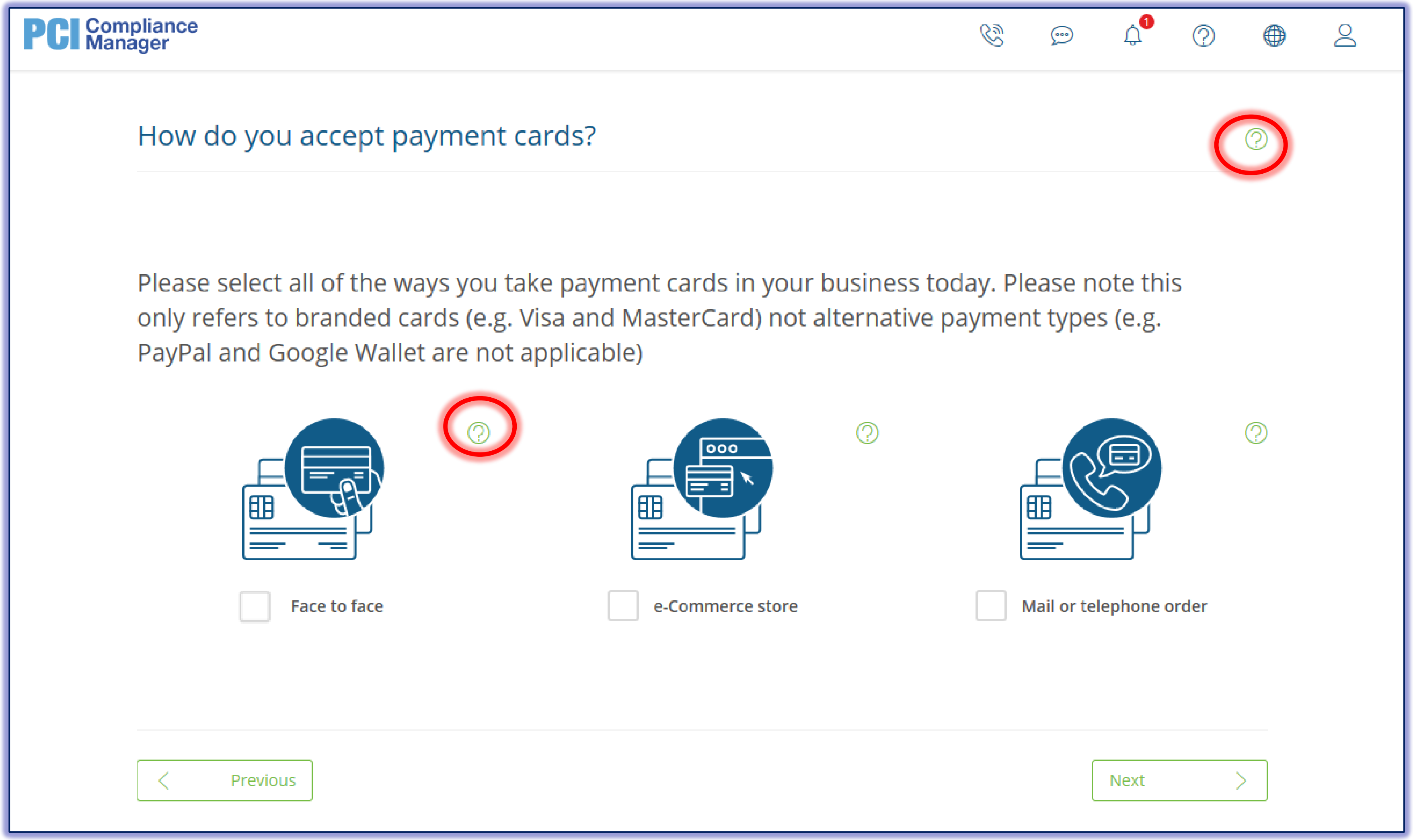
Before you begin

Have you already completed a PCI DSS Self Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) that you would like to upload?

○ Select this option if it is your first time to go through this process, OR if you completed this process more than 12months ago.

○ Select this option to upload your existing currently valid PCI DSS Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) from an external programme.

Acceptance



How do you accept payment cards?

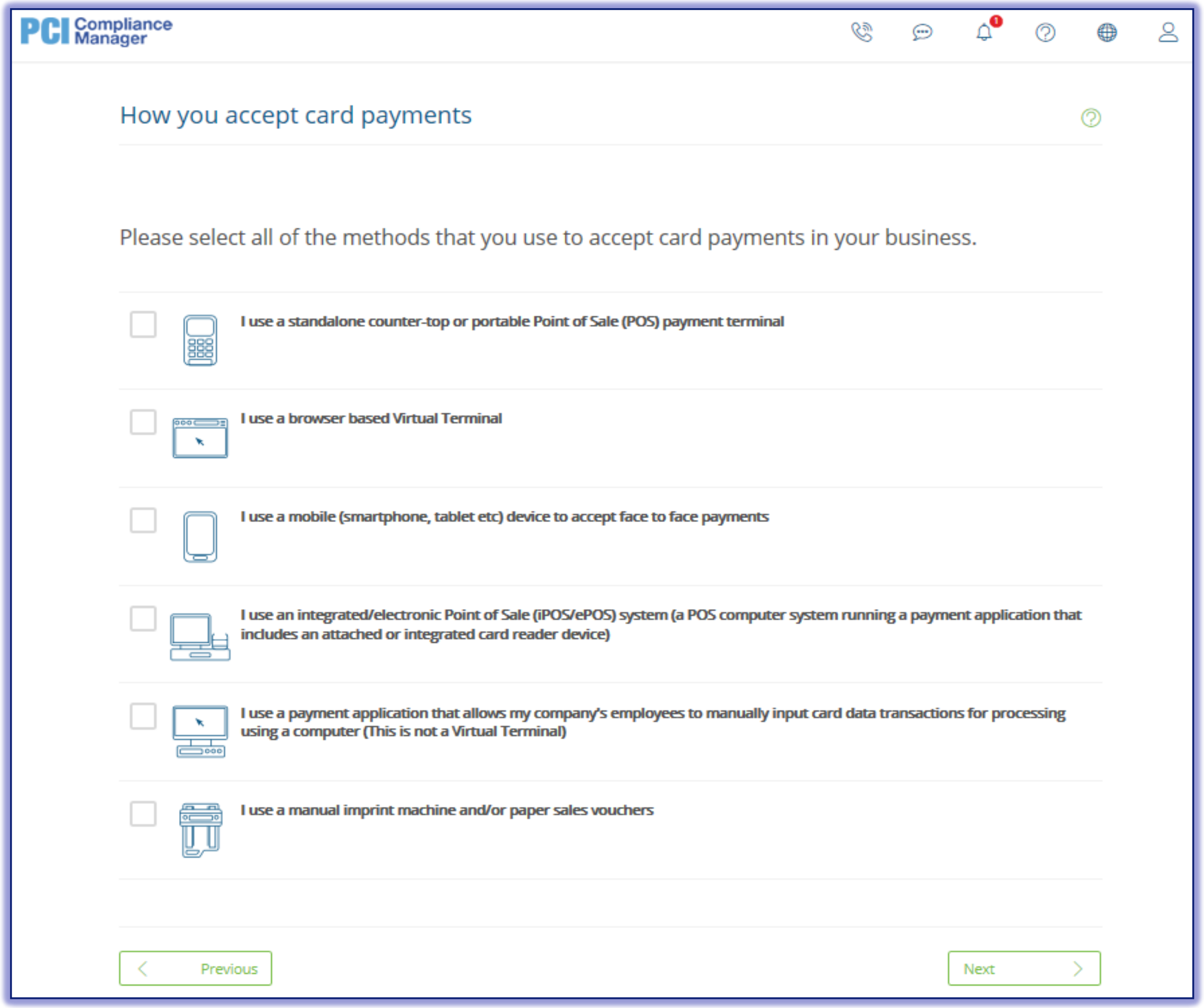
Please select all of the ways you take payment cards in your business today. Please note this only refers to branded cards (e.g. Visa and MasterCard) not alternative payment types (e.g. PayPal and Google Wallet are not applicable)

□ Face to face

□ e-Commerce store

□ Mail or telephone order

Equipment Types



How you accept card payments

Please select all of the methods that you use to accept card payments in your business.

□ I use a standalone counter-top or portable Point of Sale (POS) payment terminal

□ I use a browser based Virtual Terminal

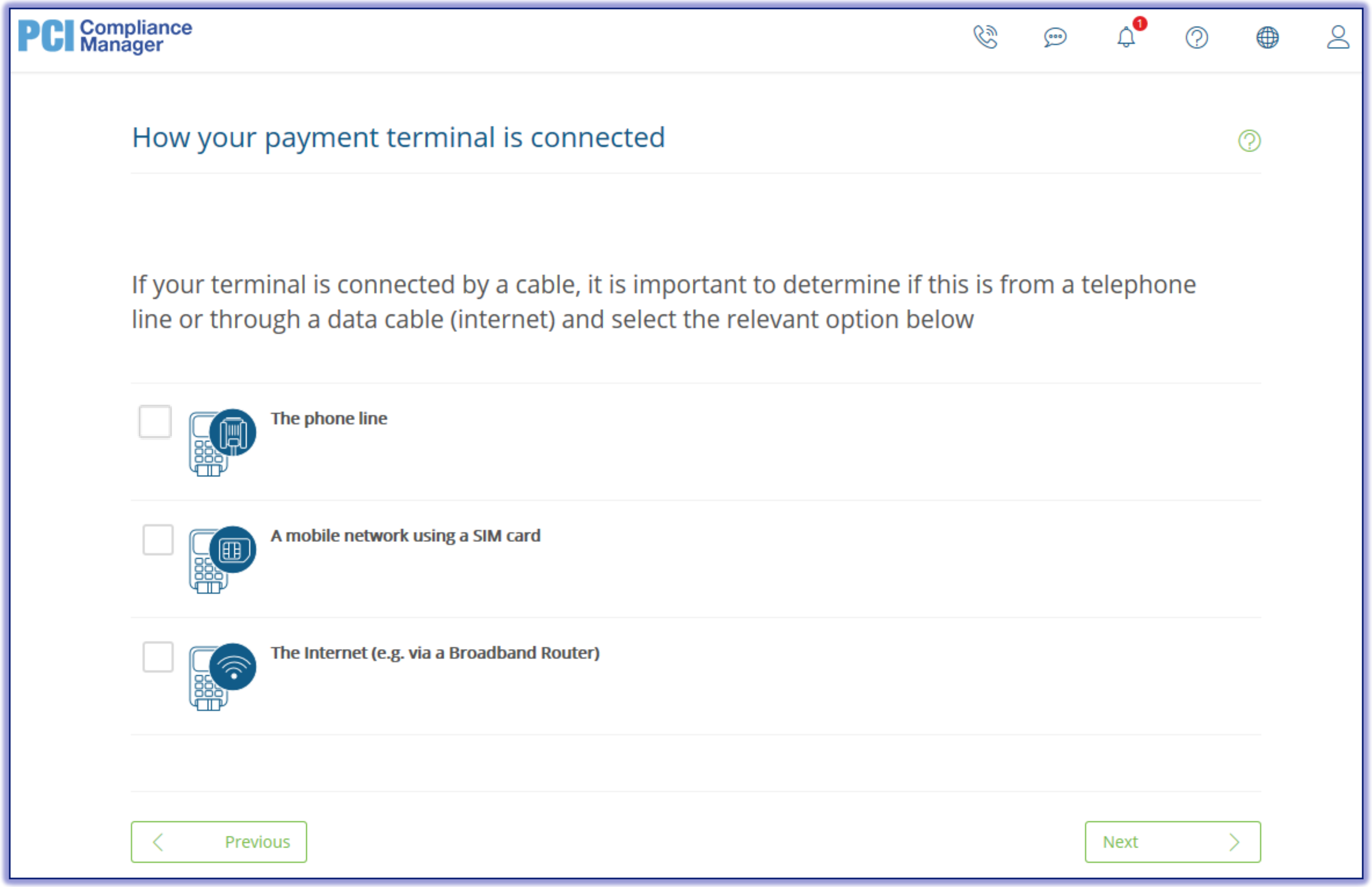
□ I use a mobile (smartphone, tablet etc) device to accept face to face payments

□ I use an integrated/electronic Point of Sale (iPOS/ePOS) system (a POS computer system running a payment application that includes an attached or integrated card reader device)

□ I use a payment application that allows my company's employees to manually input card data transactions for processing using a computer (This is not a Virtual Terminal)

□ I use a manual imprint machine and/or paper sales vouchers

Connection



How your payment terminal is connected

If your terminal is connected by a cable, it is important to determine if this is from a telephone line or through a data cable (internet) and select the relevant option below

□ The phone line

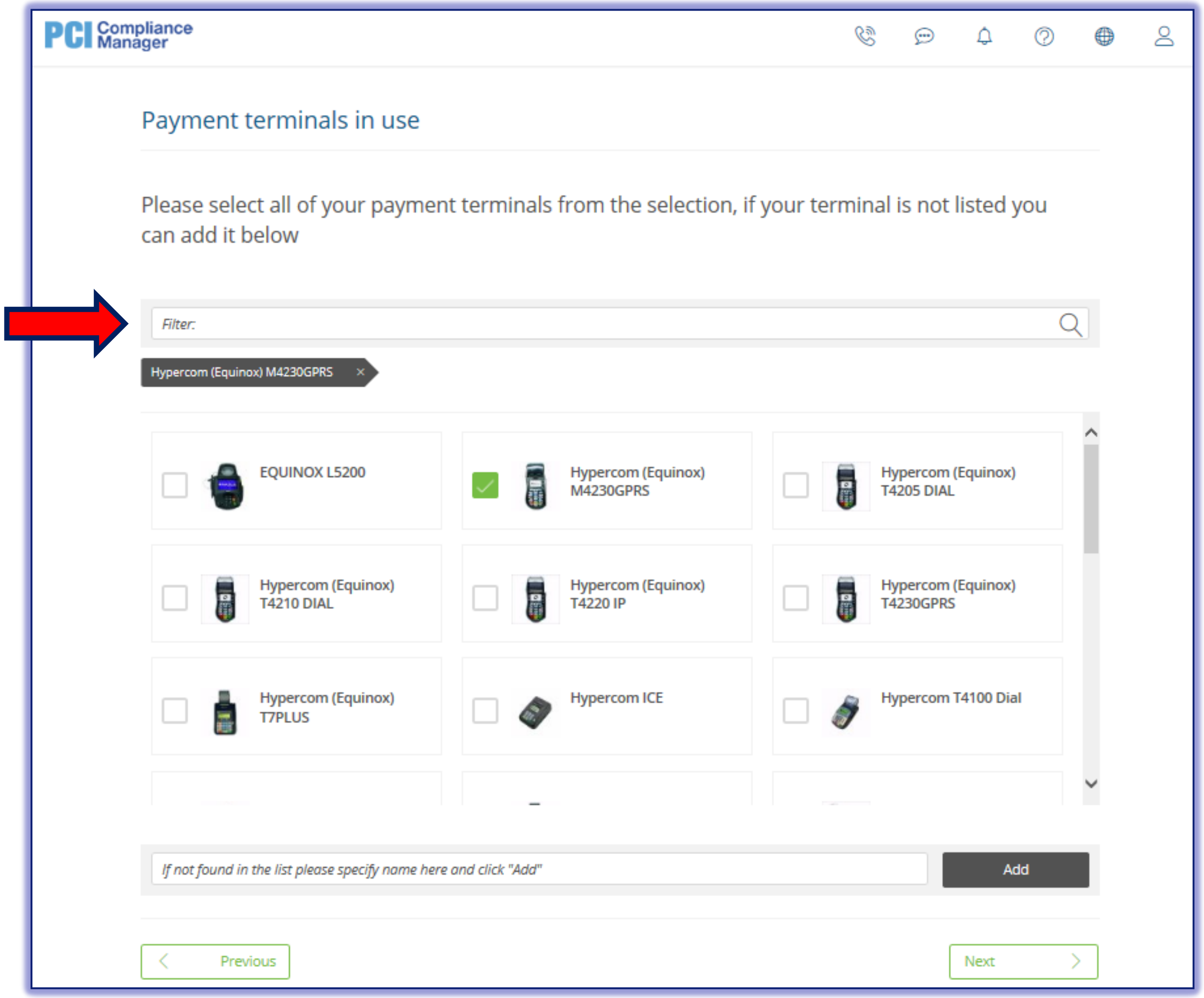
□ A mobile network using a SIM card

□ The Internet (e.g. via a Broadband Router)

< Previous

Next >

Your Equipment



PCI Compliance Manager

Payment terminals in use

Please select all of your payment terminals from the selection, if your terminal is not listed you can add it below

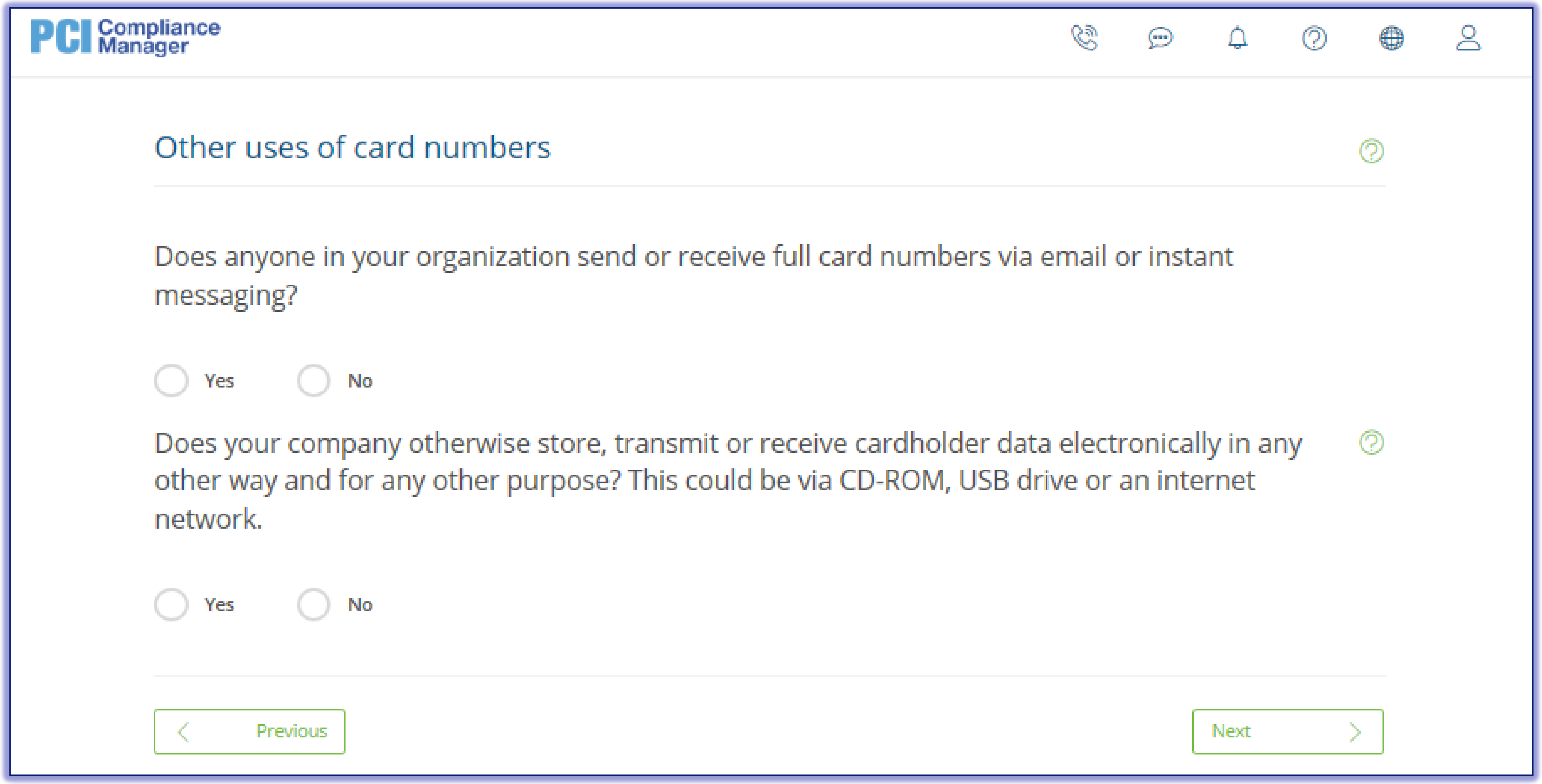
Filter:

Hypercom (Equinox) M4230GPRS ×

□ EQUINOX L5200	☑ Hypercom (Equinox) M4230GPRS	□ Hypercom (Equinox) T4205 DIAL
□ Hypercom (Equinox) T4210 DIAL	□ Hypercom (Equinox) T4220 IP	□ Hypercom (Equinox) T4230GPRS
□ Hypercom (Equinox) T7PLUS	□ Hypercom ICE	□ Hypercom T4100 Dial

If not found in the list please specify name here and click "Add"

Cardholder Data



Other uses of card numbers

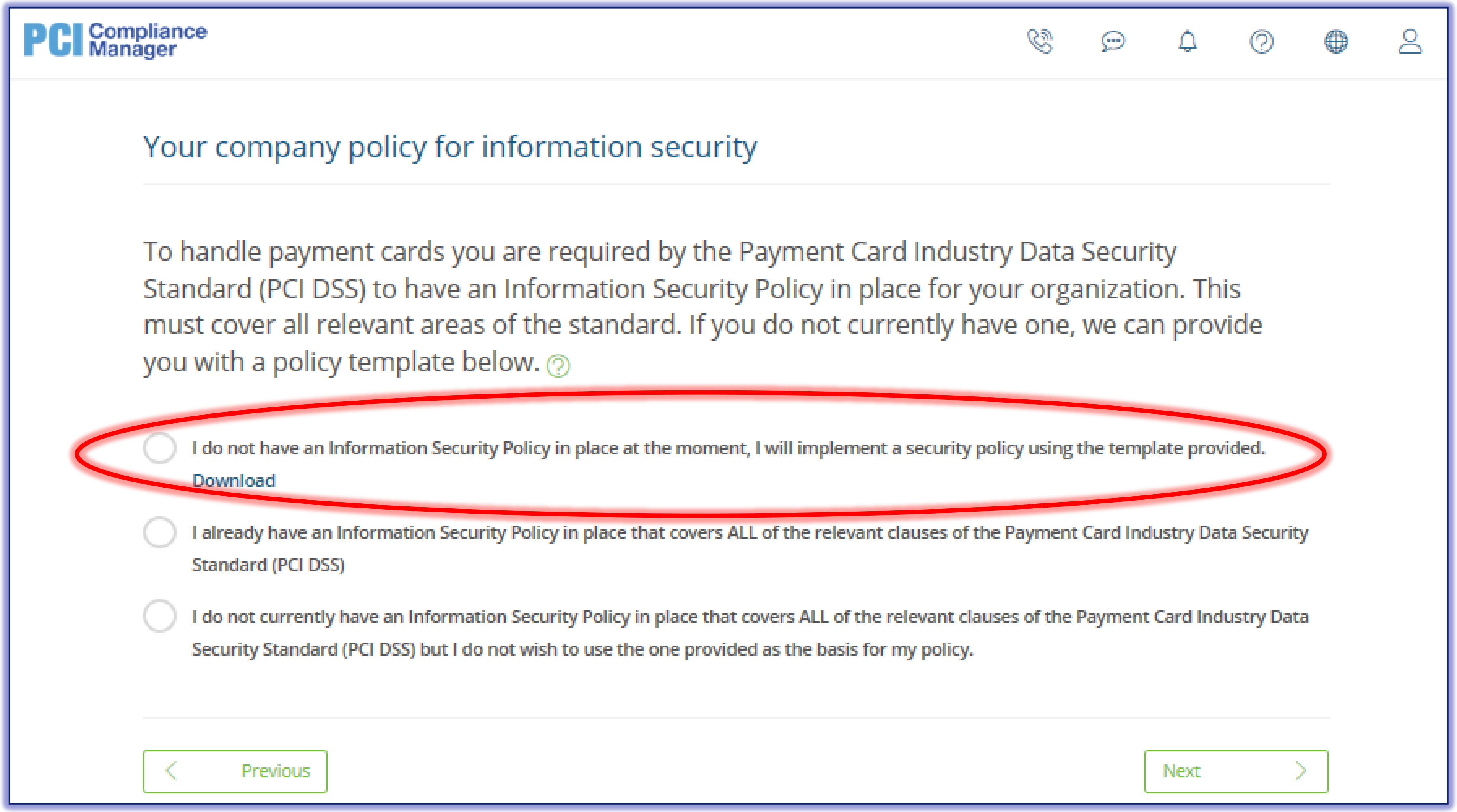
Does anyone in your organization send or receive full card numbers via email or instant messaging?

○ Yes ○ No

Does your company otherwise store, transmit or receive cardholder data electronically in any other way and for any other purpose? This could be via CD-ROM, USB drive or an internet network.

○ Yes ○ No

Security Policy



Your company policy for information security

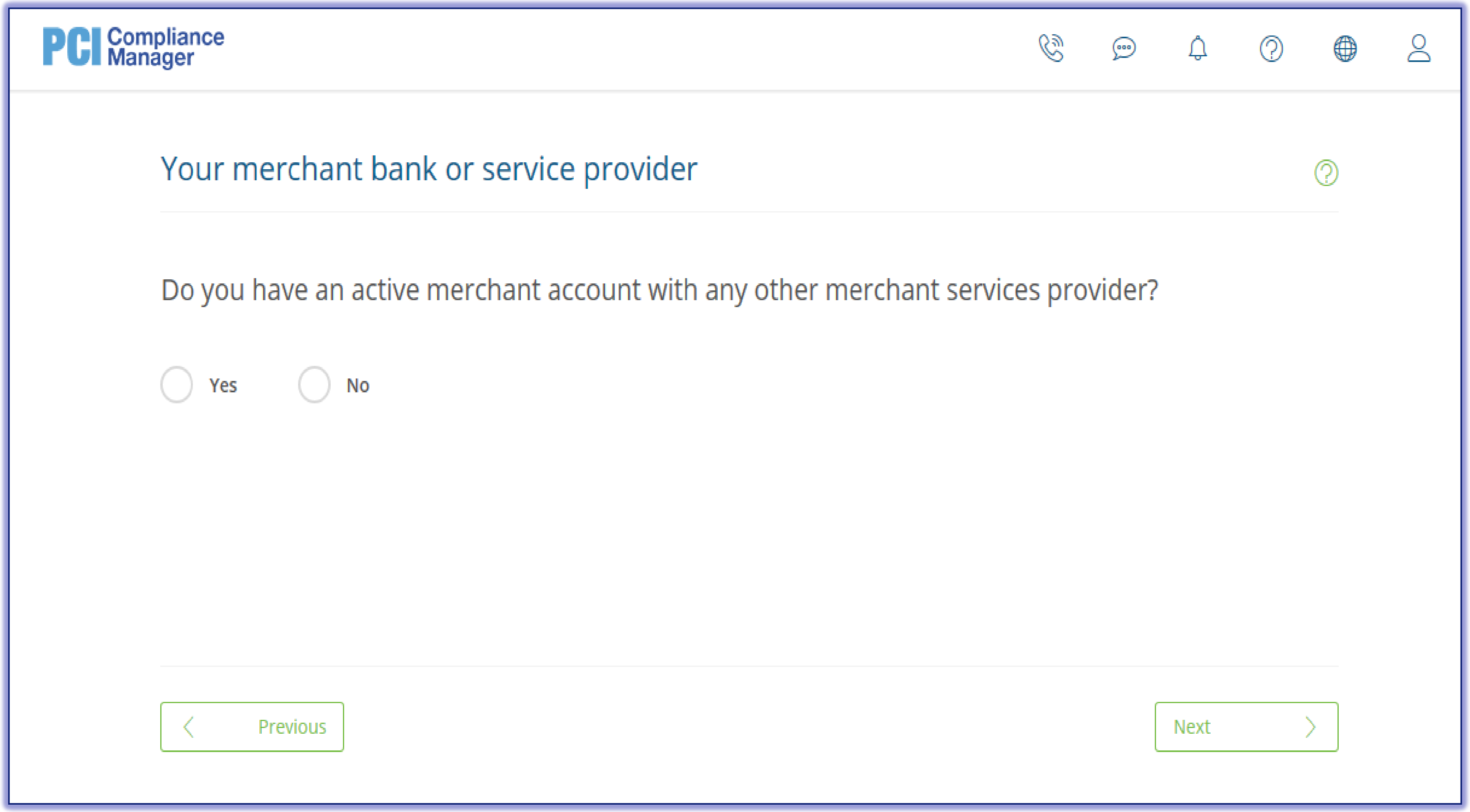
To handle payment cards you are required by the Payment Card Industry Data Security Standard (PCI DSS) to have an Information Security Policy in place for your organization. This must cover all relevant areas of the standard. If you do not currently have one, we can provide you with a policy template below.

○ I do not have an Information Security Policy in place at the moment, I will implement a security policy using the template provided.
Download

○ I already have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS)

○ I do not currently have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS) but I do not wish to use the one provided as the basis for my policy.

Merchant account

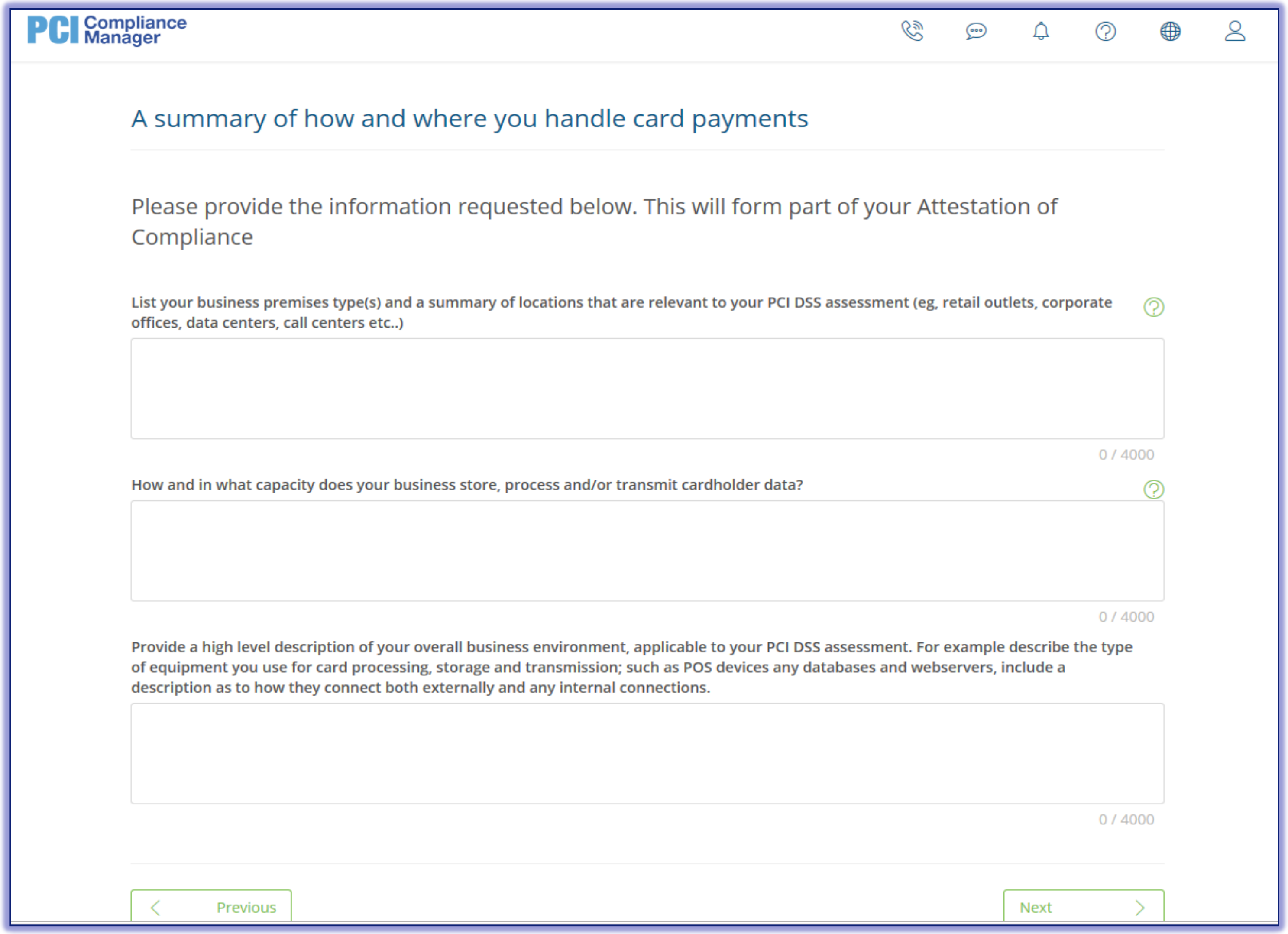


Your merchant bank or service provider

Do you have an active merchant account with any other merchant services provider?

○ Yes ○ No

Summary



A summary of how and where you handle card payments

Please provide the information requested below. This will form part of your Attestation of Compliance

List your business premises type(s) and a summary of locations that are relevant to your PCI DSS assessment (eg, retail outlets, corporate offices, data centers, call centers etc..)

0 / 4000

How and in what capacity does your business store, process and/or transmit cardholder data?

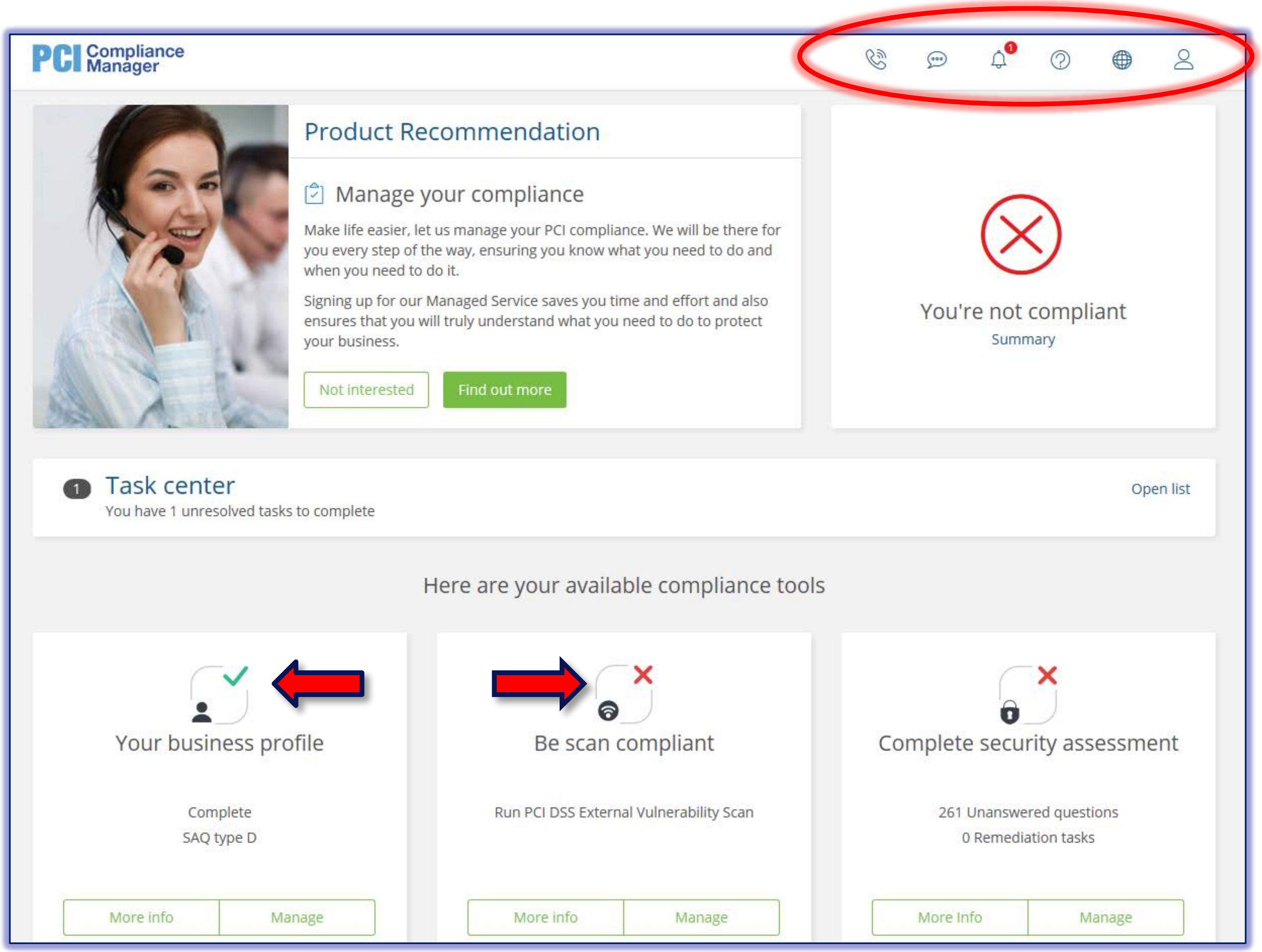
0 / 4000

Provide a high level description of your overall business environment, applicable to your PCI DSS assessment. For example describe the type of equipment you use for card processing, storage and transmission; such as POS devices any databases and webservers, include a description as to how they connect both externally and any internal connections.

0 / 4000

Main Page

Status Markers



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

Not interested | Find out more

You're not compliant

Summary

Task center

You have 1 unresolved tasks to complete

Open list

Here are your available compliance tools

Your business profile

Complete

SAQ type D

More info | Manage

Be scan compliant

Run PCI DSS External Vulnerability Scan

More info | Manage

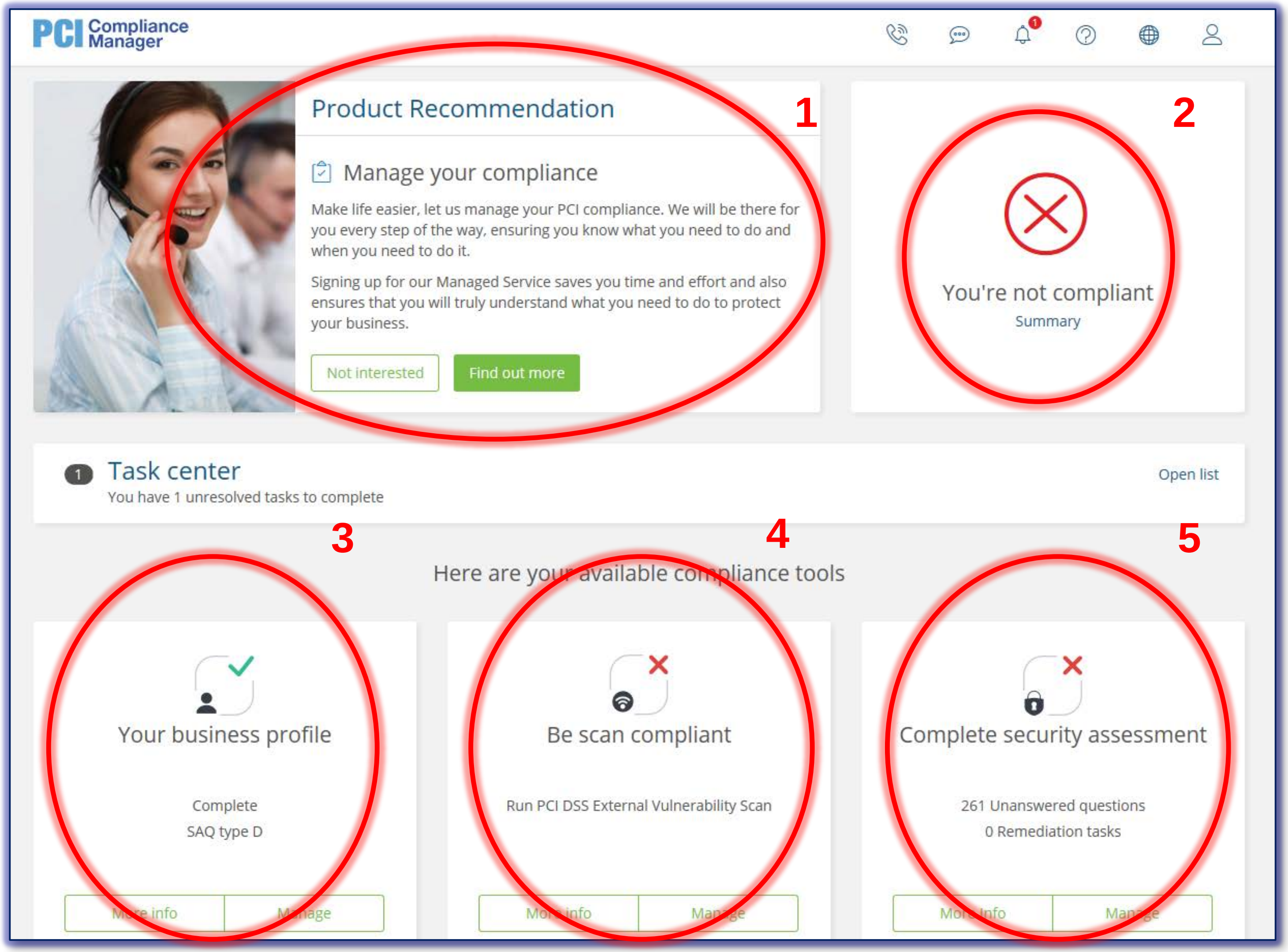
Complete security assessment

261 Unanswered questions

0 Remediation tasks

More Info | Manage

Tasks



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

Not interested | Find out more

You're not compliant

Summary

1 Task center

You have 1 unresolved tasks to complete

Open list

Here are your available compliance tools

Your business profile

Complete

SAQ type D

More info | Manage

Be scan compliant

Run PCI DSS External Vulnerability Scan

More info | Manage

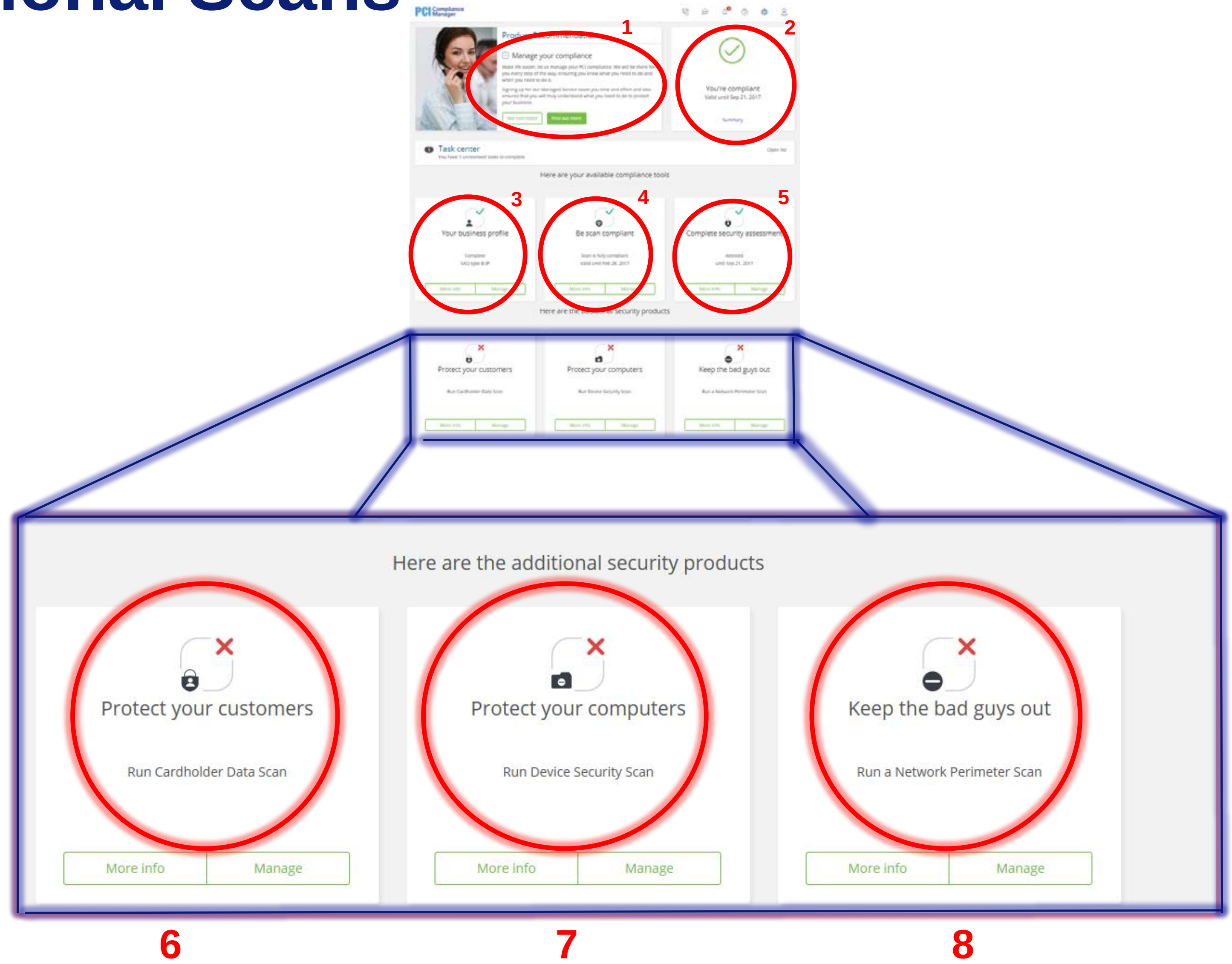
Complete security assessment

261 Unanswered questions

0 Remediation tasks

More info | Manage

Additional Scans



PCI Compliance Manager

Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

You're compliant
Valid until Sep 21, 2017

Task center
You have 1 unresolved tasks to complete

Here are your available compliance tools

Your business profile
Complete
SAQ type B-IP

Be scan compliant
Scan is fully compliant
valid until Feb 28, 2017

Complete security assessment
Attested
until Sep 21, 2017

Here are the additional security products

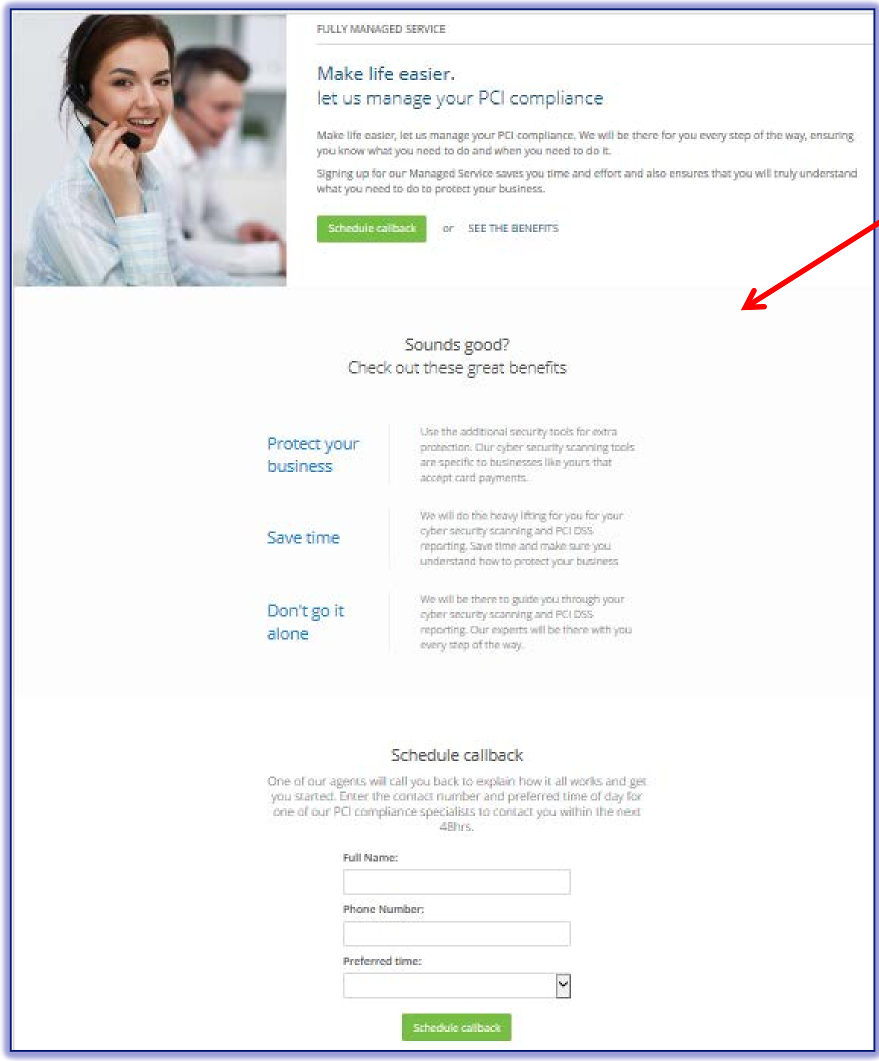
Protect your customers
Run Cardholder Data Scan

Protect your computers
Run Device Security Scan

Keep the bad guys out
Run a Network Perimeter Scan

Closer Look

Product Recommendation



FULLY MANAGED SERVICE

Make life easier.
let us manage your PCI compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

Schedule callback or SEE THE BENEFITS

Sounds good?
Check out these great benefits

Protect your business — Use the additional security tools for extra protection. Our cyber security scanning tools are specific to businesses like yours that accept card payments.

Save time — We will do the heavy lifting for you for your cyber security scanning and PCI DSS reporting. Save time and make sure you understand how to protect your business.

Don't go it alone — We will be there to guide you through your cyber security scanning and PCI DSS reporting. Our experts will be there with you every step of the way.

Schedule callback

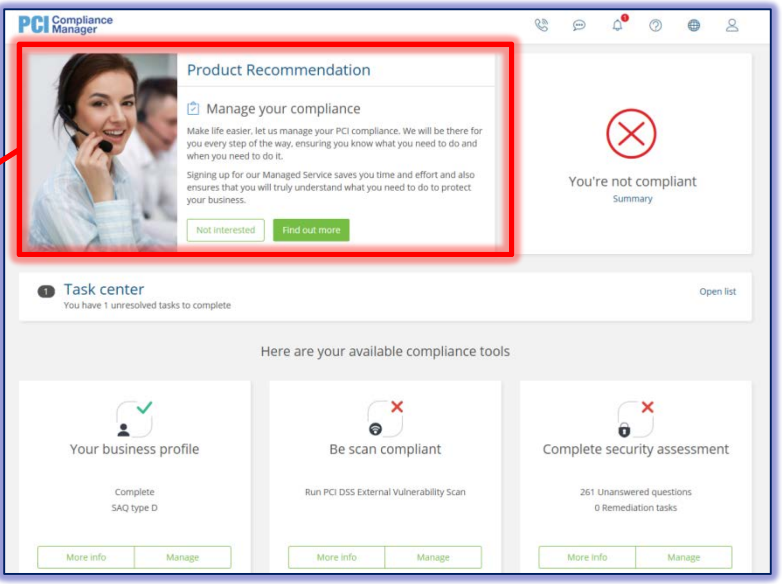
One of our agents will call you back to explain how it all works and get you started. Enter the contact number and preferred time of day for one of our PCI compliance specialists to contact you within the next 48hrs.

Full Name:

Phone Number:

Preferred time:

Schedule callback



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

Not interested | Find out more

You're not compliant
Summary

Task center
You have 1 unresolved tasks to complete
Open list

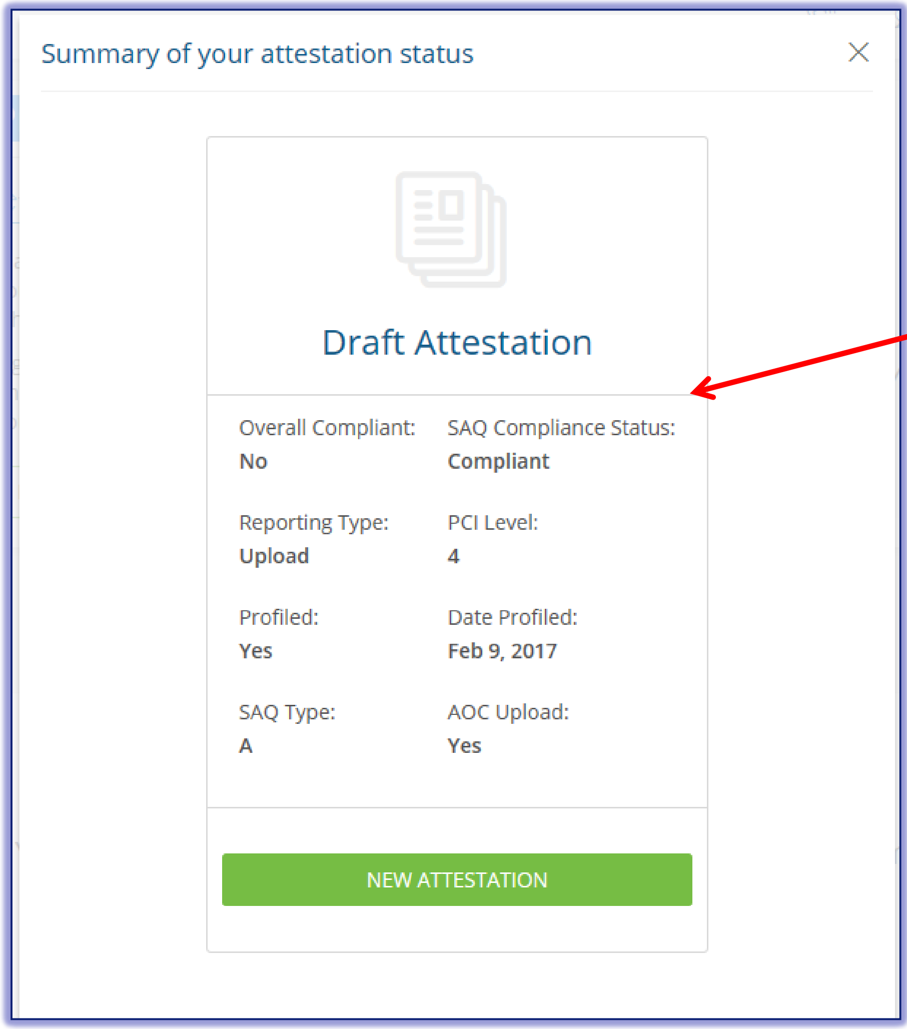
Here are your available compliance tools

Your business profile
Complete
SAQ type D
More info | Manage

Be scan compliant
Run PCI DSS External Vulnerability Scan
More info | Manage

Complete security assessment
261 Unanswered questions
0 Remediation tasks
More Info | Manage

Compliance Summary



Summary of your attestation status

Draft Attestation

Overall Compliant:
No

SAQ Compliance Status:
Compliant

Reporting Type:
Upload

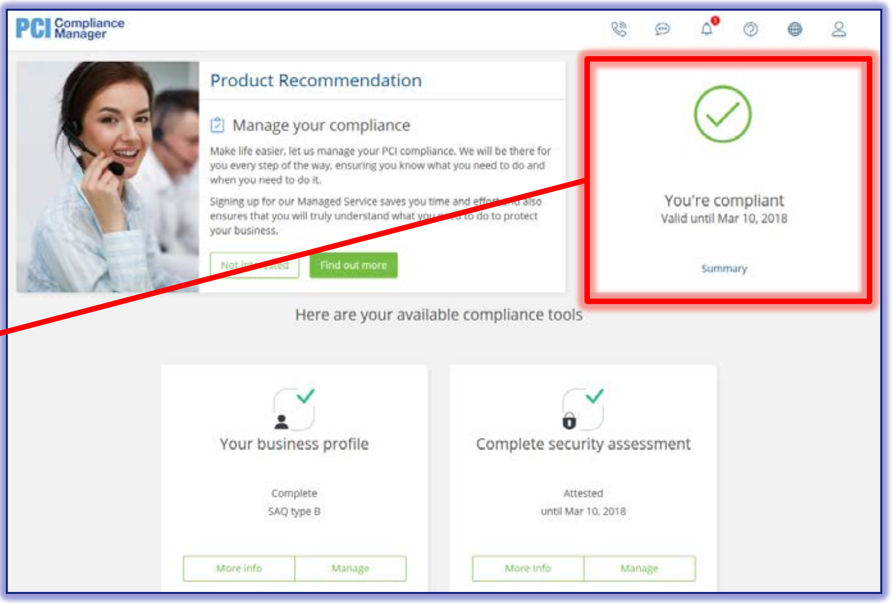
PCI Level:
4

Profiled:
Yes

Date Profiled:
Feb 9, 2017

SAQ Type:
A

AOC Upload:
Yes



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

You're compliant
Valid until Mar 10, 2018

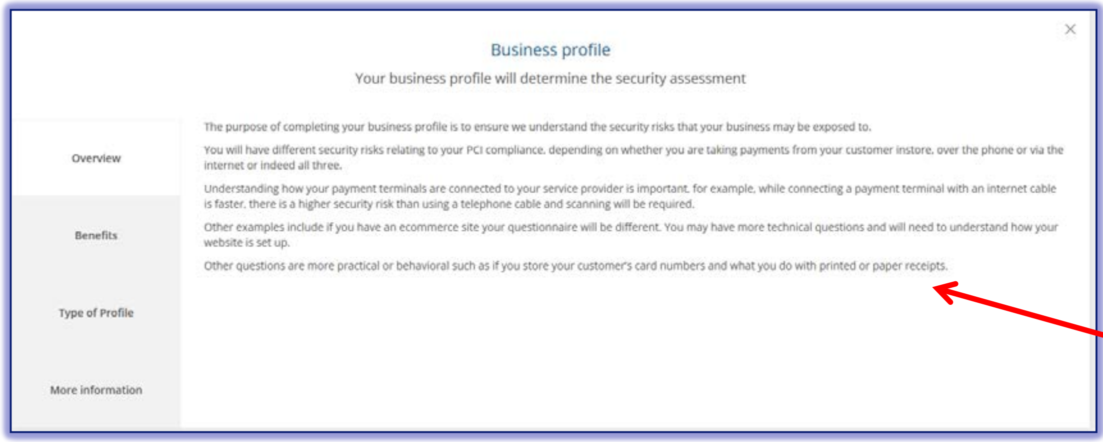
Here are your available compliance tools

Your business profile
Complete
SAQ type B

Complete security assessment
Attested
until Mar 10, 2018

Business Profile

More Info



Business profile

Your business profile will determine the security assessment

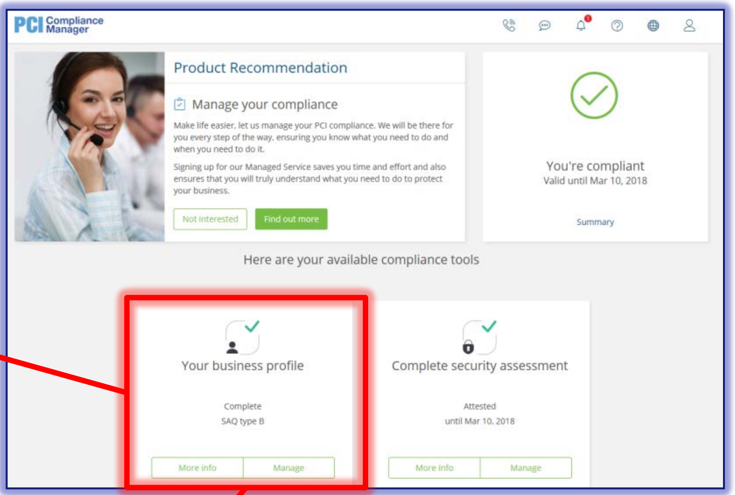
The purpose of completing your business profile is to ensure we understand the security risks that your business may be exposed to.

You will have different security risks relating to your PCI compliance. depending on whether you are taking payments from your customer instore, over the phone or via the internet or indeed all three.

Understanding how your payment terminals are connected to your service provider is important. for example, while connecting a payment terminal with an internet cable is faster, there is a higher security risk than using a telephone cable and scanning will be required.

Other examples include if you have an ecommerce site your questionnaire will be different. You may have more technical questions and will need to understand how your website is set up.

Other questions are more practical or behavioral such as if you store your customer's card numbers and what you do with printed or paper receipts.



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

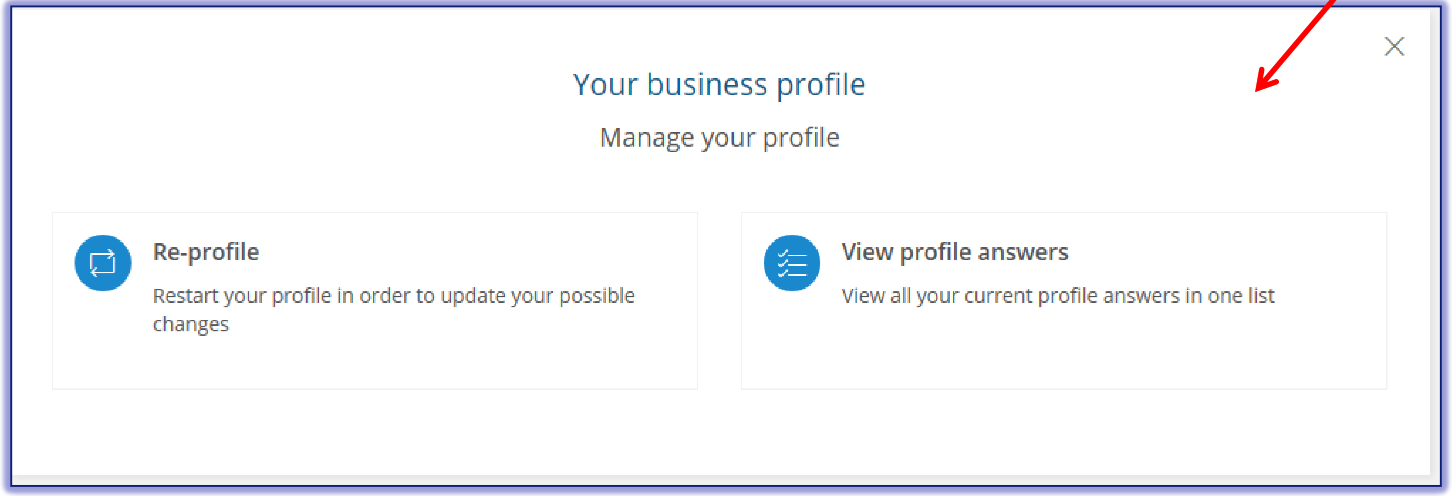
You're compliant
Valid until Mar 10, 2018

Here are your available compliance tools

Your business profile
Complete
SAQ type B

Complete security assessment
Attested
until Mar 10, 2018

Manage



Your business profile

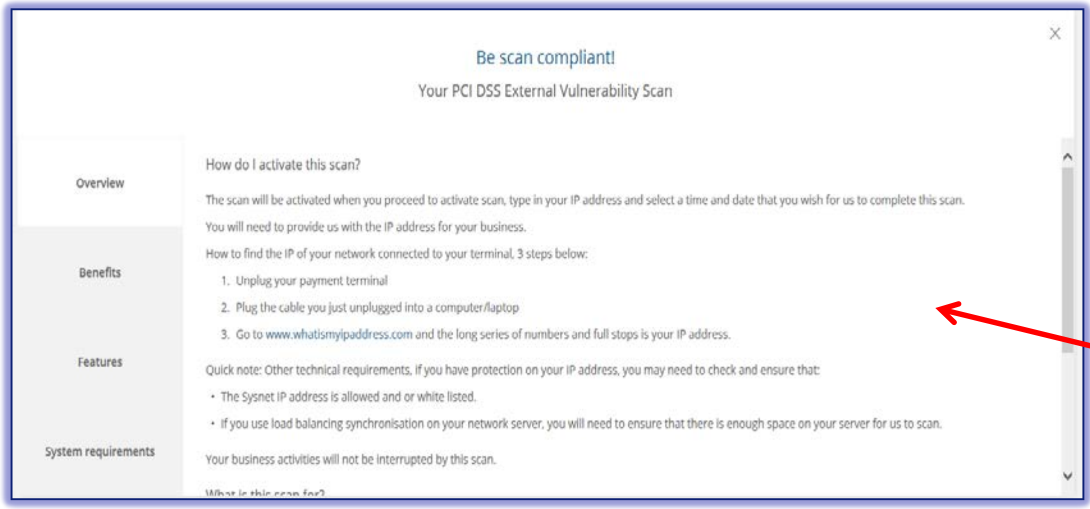
Manage your profile

Re-profile
Restart your profile in order to update your possible changes

View profile answers
View all your current profile answers in one list

Scan Compliance

More Info


Be scan compliant!

Your PCI DSS External Vulnerability Scan

How do I activate this scan?

The scan will be activated when you proceed to activate scan, type in your IP address and select a time and date that you wish for us to complete this scan.

You will need to provide us with the IP address for your business.

How to find the IP of your network connected to your terminal, 3 steps below:

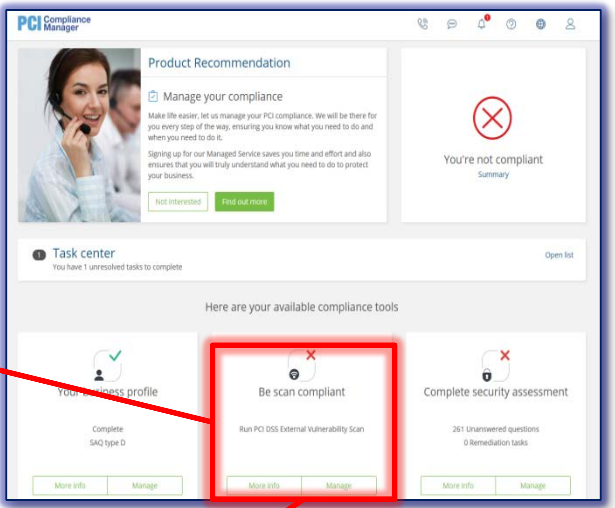
1. Unplug your payment terminal
2. Plug the cable you just unplugged into a computer/laptop
3. Go to www.whatismyipaddress.com and the long series of numbers and full stops is your IP address.

Quick note: Other technical requirements, If you have protection on your IP address, you may need to check and ensure that:

- The Sysnet IP address is allowed and or white listed.
- If you use load balancing synchronisation on your network server, you will need to ensure that there is enough space on your server for us to scan.

Your business activities will not be interrupted by this scan.

What is this scan for?



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

You're not compliant

Task center

You have 1 unresolved tasks to complete

Here are your available compliance tools

Your business profile

Complete

SAQ type D

Be scan compliant

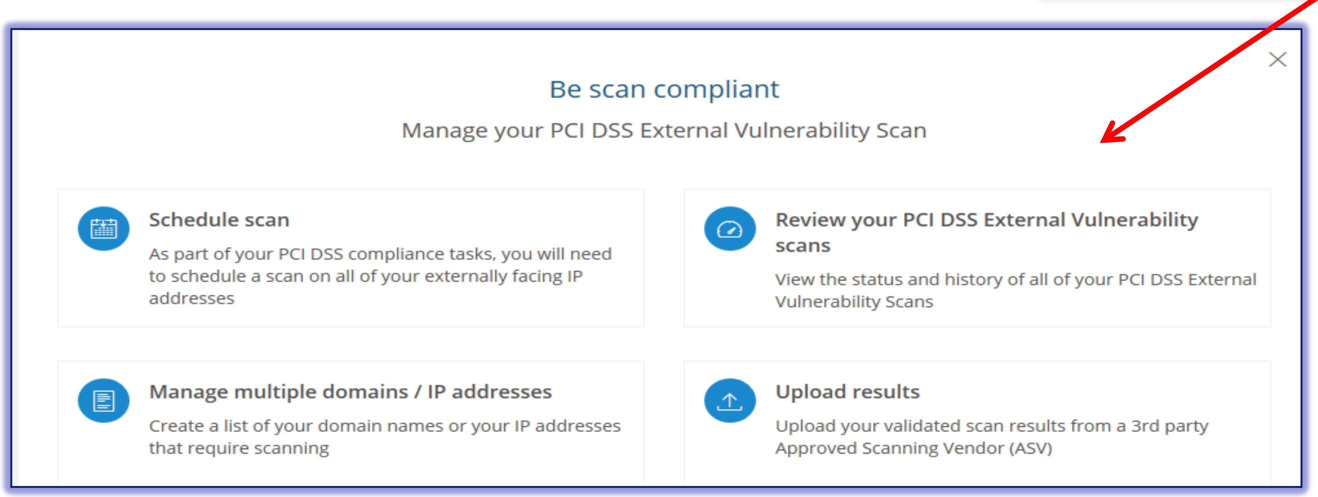
Run PCI DSS External Vulnerability Scan

Complete security assessment

261 Unanswered questions

0 Remediation tasks

Manage


Be scan compliant

Manage your PCI DSS External Vulnerability Scan

Schedule scan

As part of your PCI DSS compliance tasks, you will need to schedule a scan on all of your externally facing IP addresses

Review your PCI DSS External Vulnerability scans

View the status and history of all of your PCI DSS External Vulnerability Scans

Manage multiple domains / IP addresses

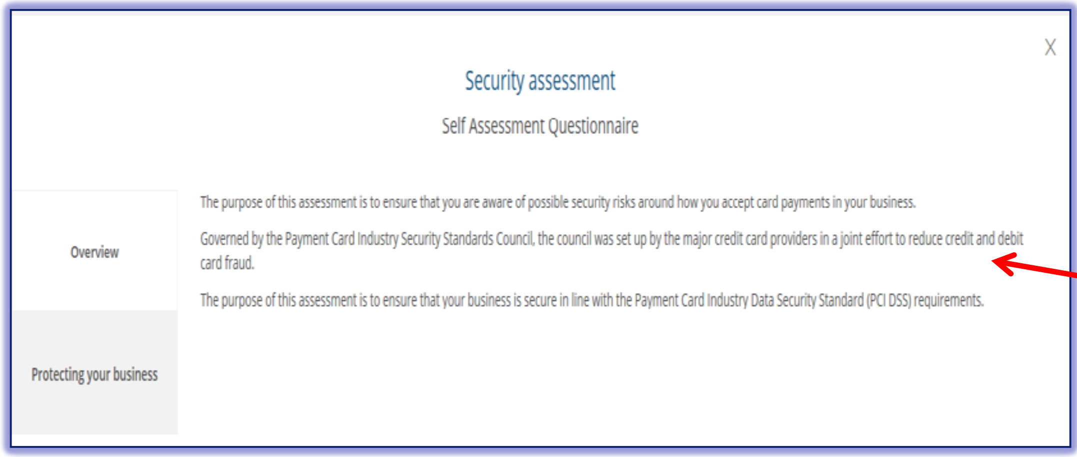
Create a list of your domain names or your IP addresses that require scanning

Upload results

Upload your validated scan results from a 3rd party Approved Scanning Vendor (ASV)

Security Assessment

More Info



X

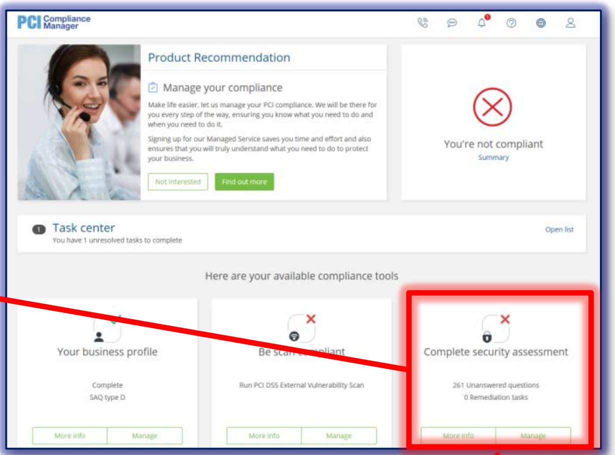
Security assessment

Self Assessment Questionnaire

The purpose of this assessment is to ensure that you are aware of possible security risks around how you accept card payments in your business.

Governed by the Payment Card Industry Security Standards Council, the council was set up by the major credit card providers in a joint effort to reduce credit and debit card fraud.

The purpose of this assessment is to ensure that your business is secure in line with the Payment Card Industry Data Security Standard (PCI DSS) requirements.



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

You're not compliant

Task center

You have 1 unresolved tasks to complete

Here are your available compliance tools

Your business profile

Complete
SAQ type D

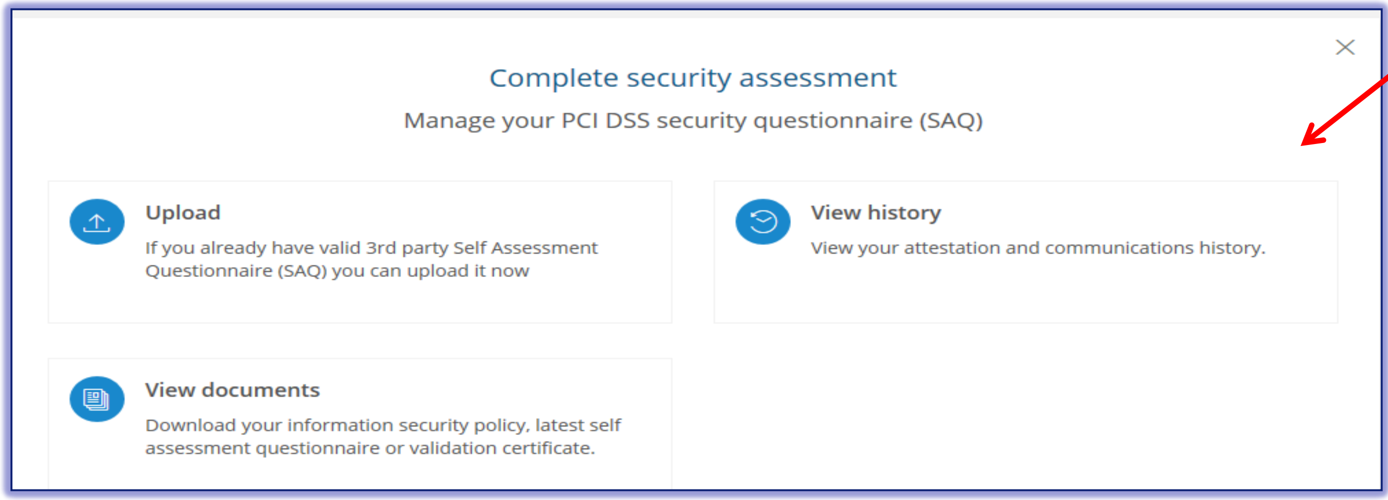
Be scan compliant

Run PCI DSS External Vulnerability Scan

Complete security assessment

261 Unanswered questions
0 Remediation tasks

Manage



Complete security assessment

Manage your PCI DSS security questionnaire (SAQ)

Upload

If you already have valid 3rd party Self Assessment Questionnaire (SAQ) you can upload it now

View history

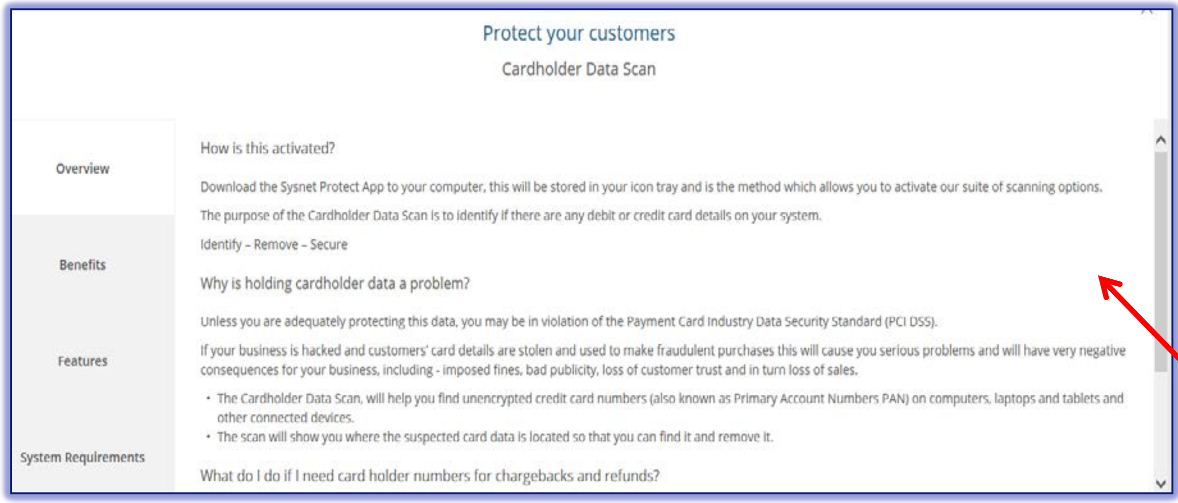
View your attestation and communications history.

View documents

Download your information security policy, latest self assessment questionnaire or validation certificate.

Cardholder Data Scan

More Info



Protect your customers

Cardholder Data Scan

How is this activated?

Download the Sysnet Protect App to your computer, this will be stored in your icon tray and is the method which allows you to activate our suite of scanning options.

The purpose of the Cardholder Data Scan is to identify if there are any debit or credit card details on your system.

Identify – Remove – Secure

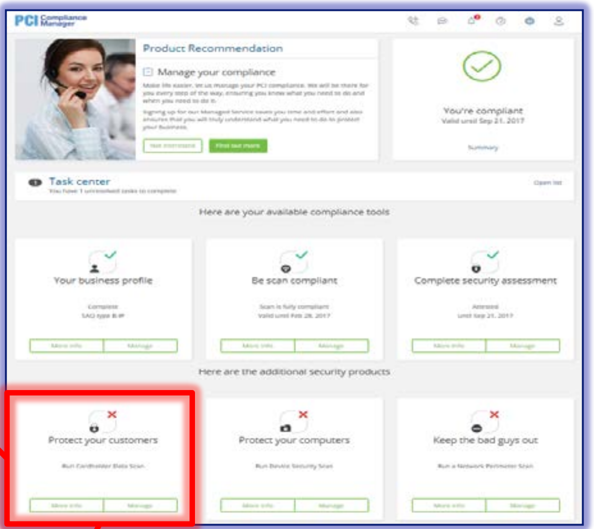
Why is holding cardholder data a problem?

Unless you are adequately protecting this data, you may be in violation of the Payment Card Industry Data Security Standard (PCI DSS).

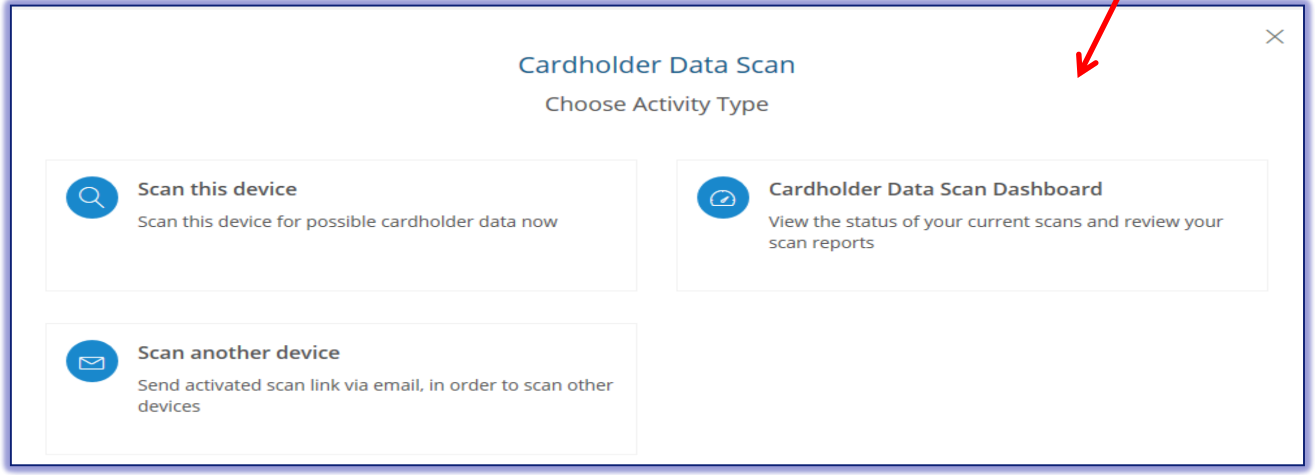
If your business is hacked and customers' card details are stolen and used to make fraudulent purchases this will cause you serious problems and will have very negative consequences for your business, including - imposed fines, bad publicity, loss of customer trust and in turn loss of sales.

- The Cardholder Data Scan, will help you find unencrypted credit card numbers (also known as Primary Account Numbers PAN) on computers, laptops and tablets and other connected devices.
- The scan will show you where the suspected card data is located so that you can find it and remove it.

What do I do if I need card holder numbers for chargebacks and refunds?



Manage



Cardholder Data Scan

Choose Activity Type

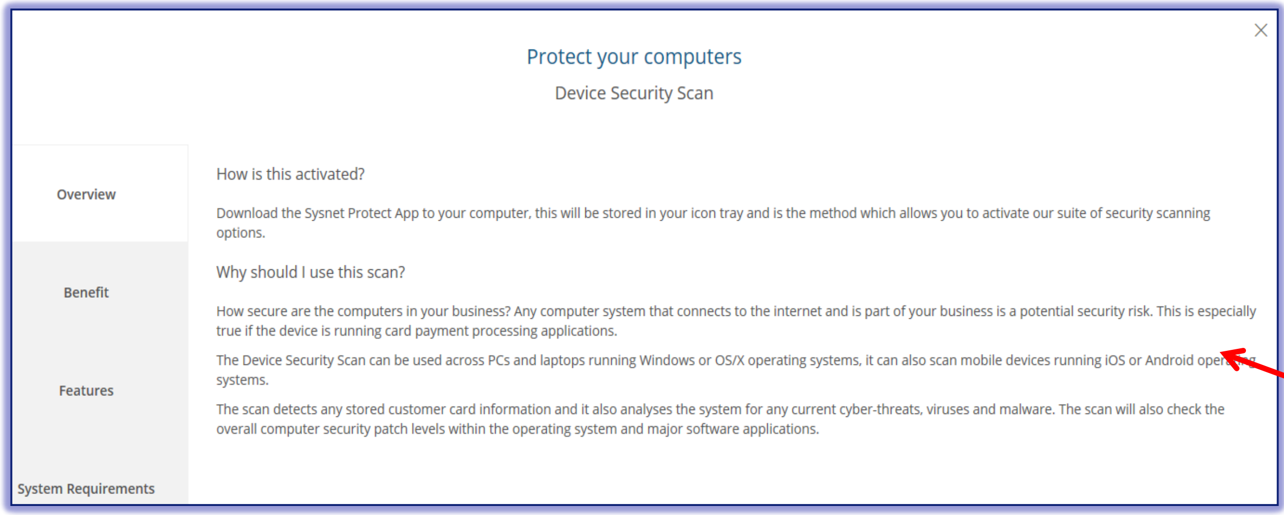
Scan this device
Scan this device for possible cardholder data now

Cardholder Data Scan Dashboard
View the status of your current scans and review your scan reports

Scan another device
Send activated scan link via email, in order to scan other devices

Device Security Scan

More Info



Protect your computers

Device Security Scan

How is this activated?

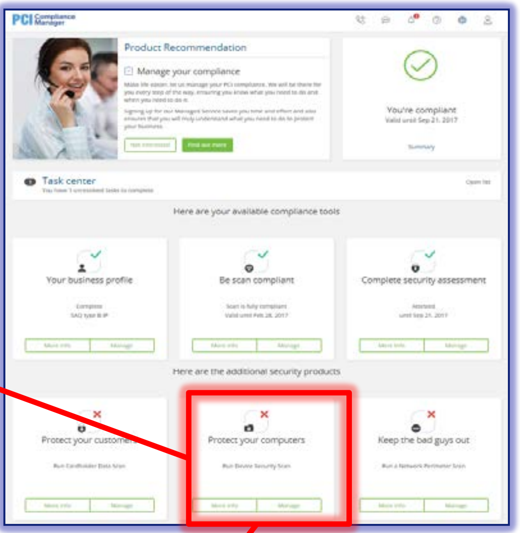
Download the Sysnet Protect App to your computer, this will be stored in your icon tray and is the method which allows you to activate our suite of security scanning options.

Why should I use this scan?

How secure are the computers in your business? Any computer system that connects to the internet and is part of your business is a potential security risk. This is especially true if the device is running card payment processing applications.

The Device Security Scan can be used across PCs and laptops running Windows or OS/X operating systems, it can also scan mobile devices running iOS or Android operating systems.

The scan detects any stored customer card information and it also analyses the system for any current cyber-threats, viruses and malware. The scan will also check the overall computer security patch levels within the operating system and major software applications.



Product Recommendation

Manage your compliance

You're compliant
Valid until Sep 21, 2017

Task center

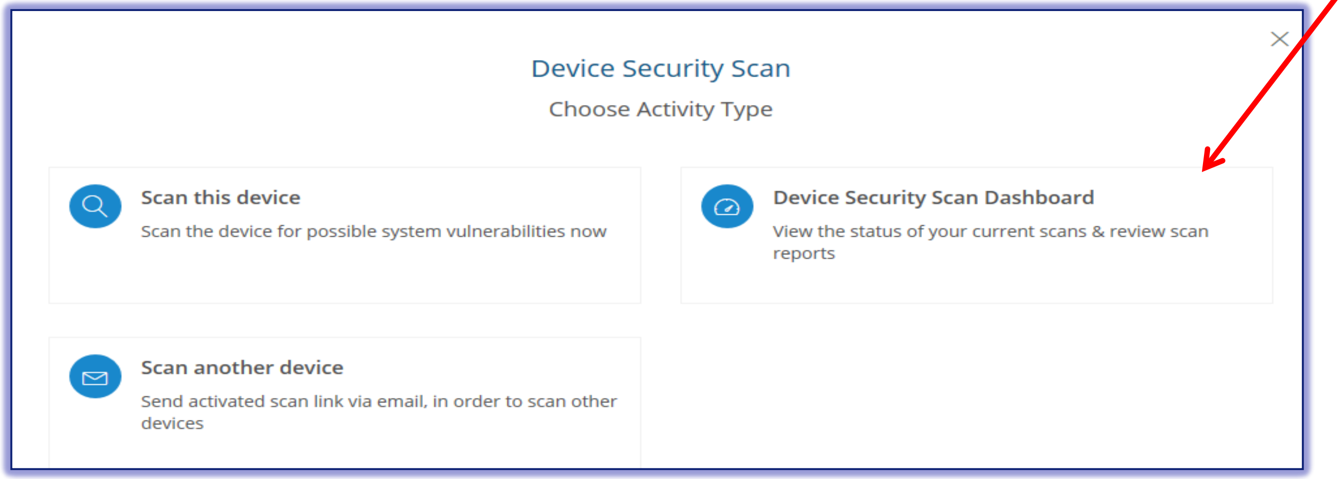
Here are your available compliance tools

Your business profile	Be scan compliant	Complete security assessment
Complete SAQ type B-IP	Scan is fully compliant Valid until Feb 28, 2017	Attested until Sep 21, 2017

Here are the additional security products

Protect your customers	Protect your computers	Keep the bad guys out
Run Cardholder Data Scan	Run Device Security Scan	Run a Network Perimeter Scan

Manage



Device Security Scan

Choose Activity Type

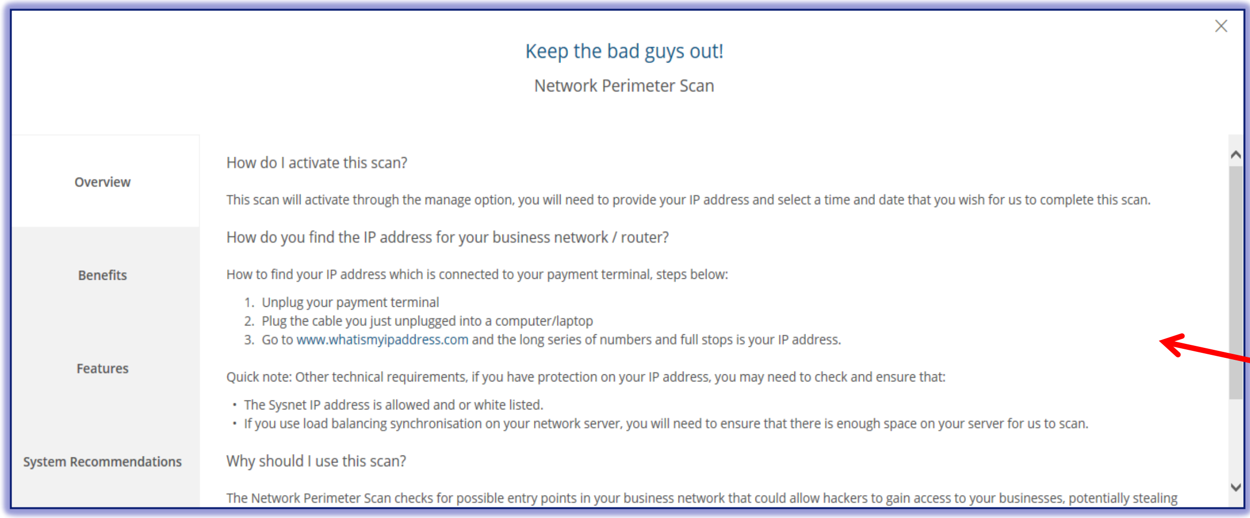
Scan this device
Scan the device for possible system vulnerabilities now

Device Security Scan Dashboard
View the status of your current scans & review scan reports

Scan another device
Send activated scan link via email, in order to scan other devices

Network Perimeter Scan

More Info



Keep the bad guys out!

Network Perimeter Scan

How do I activate this scan?

This scan will activate through the manage option, you will need to provide your IP address and select a time and date that you wish for us to complete this scan.

How do you find the IP address for your business network / router?

How to find your IP address which is connected to your payment terminal, steps below:

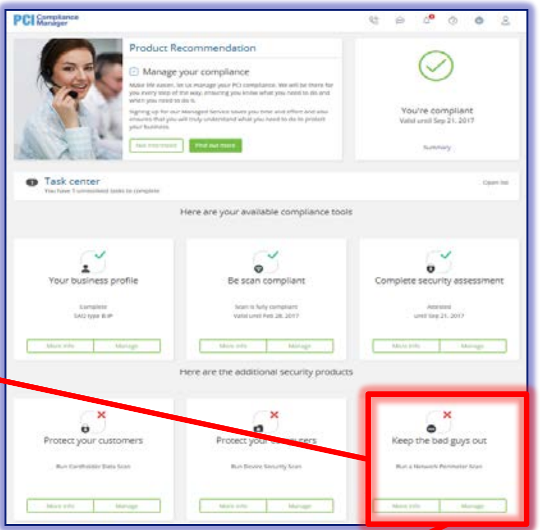
1. Unplug your payment terminal
2. Plug the cable you just unplugged into a computer/laptop
3. Go to www.whatismyipaddress.com and the long series of numbers and full stops is your IP address.

Quick note: Other technical requirements, if you have protection on your IP address, you may need to check and ensure that:

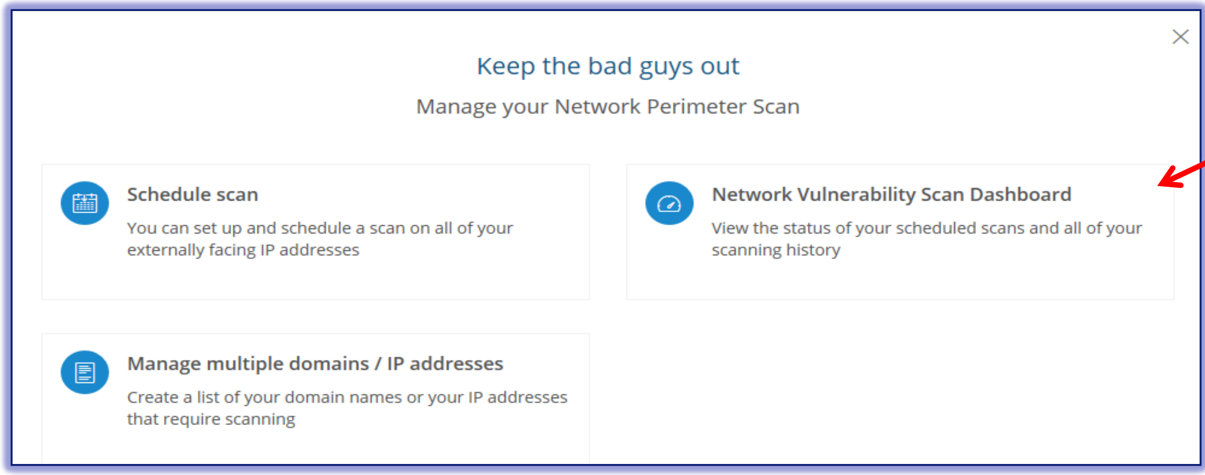
- The Sysnet IP address is allowed and or white listed.
- If you use load balancing synchronisation on your network server, you will need to ensure that there is enough space on your server for us to scan.

Why should I use this scan?

The Network Perimeter Scan checks for possible entry points in your business network that could allow hackers to gain access to your businesses, potentially stealing



Manage



Keep the bad guys out

Manage your Network Perimeter Scan

Schedule scan

You can set up and schedule a scan on all of your externally facing IP addresses

Network Vulnerability Scan Dashboard

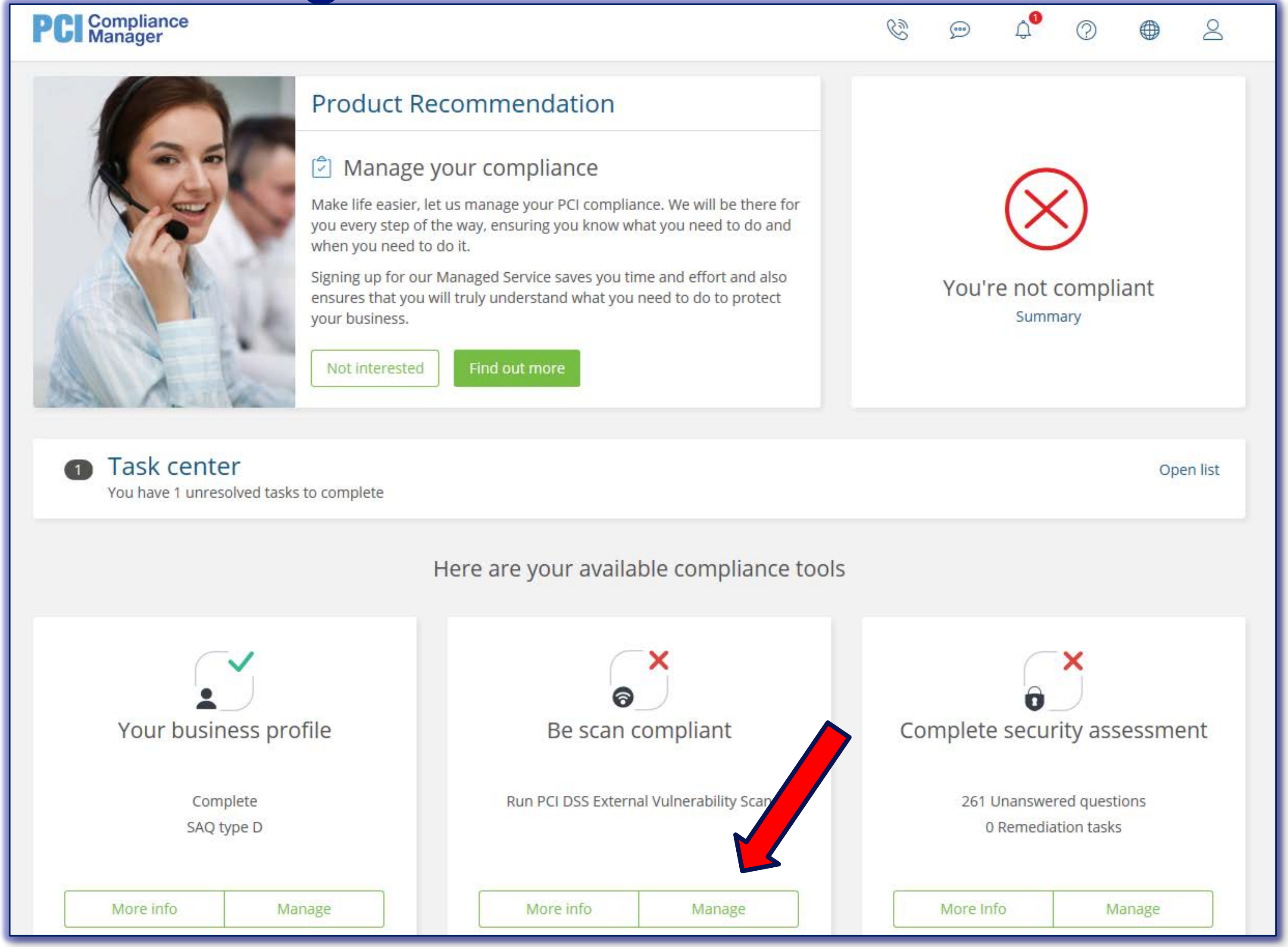
View the status of your scheduled scans and all of your scanning history

Manage multiple domains / IP addresses

Create a list of your domain names or your IP addresses that require scanning

Scan

Main Page



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

You're not compliant

Task center

You have 1 unresolved tasks to complete

Here are your available compliance tools

Your business profile

Complete

SAQ type D

Be scan compliant

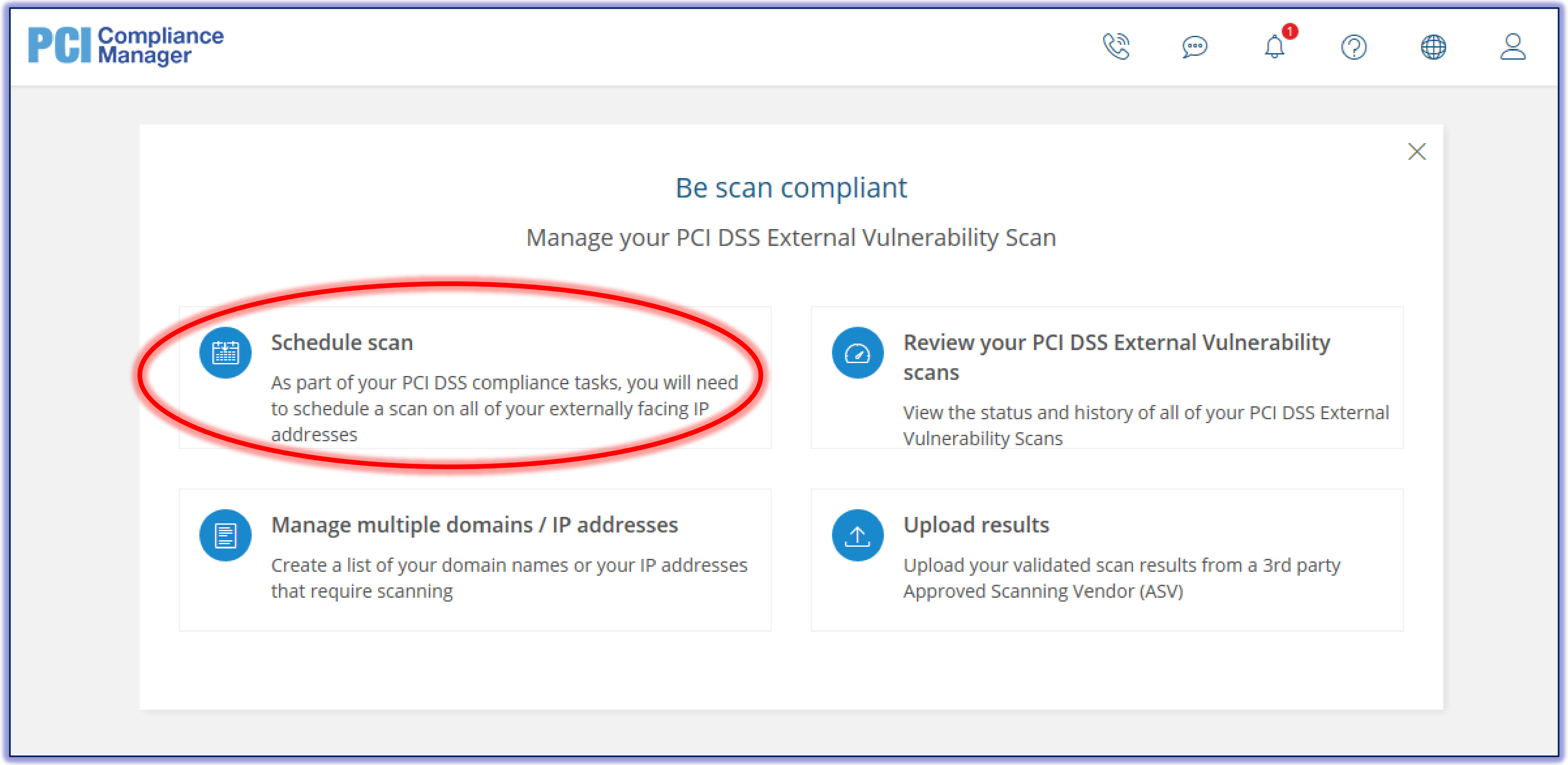
Run PCI DSS External Vulnerability Scan

Complete security assessment

261 Unanswered questions

0 Remediation tasks

Scheduling a Scan



Be scan compliant

Manage your PCI DSS External Vulnerability Scan

Schedule scan

As part of your PCI DSS compliance tasks, you will need to schedule a scan on all of your externally facing IP addresses

Review your PCI DSS External Vulnerability scans

View the status and history of all of your PCI DSS External Vulnerability Scans

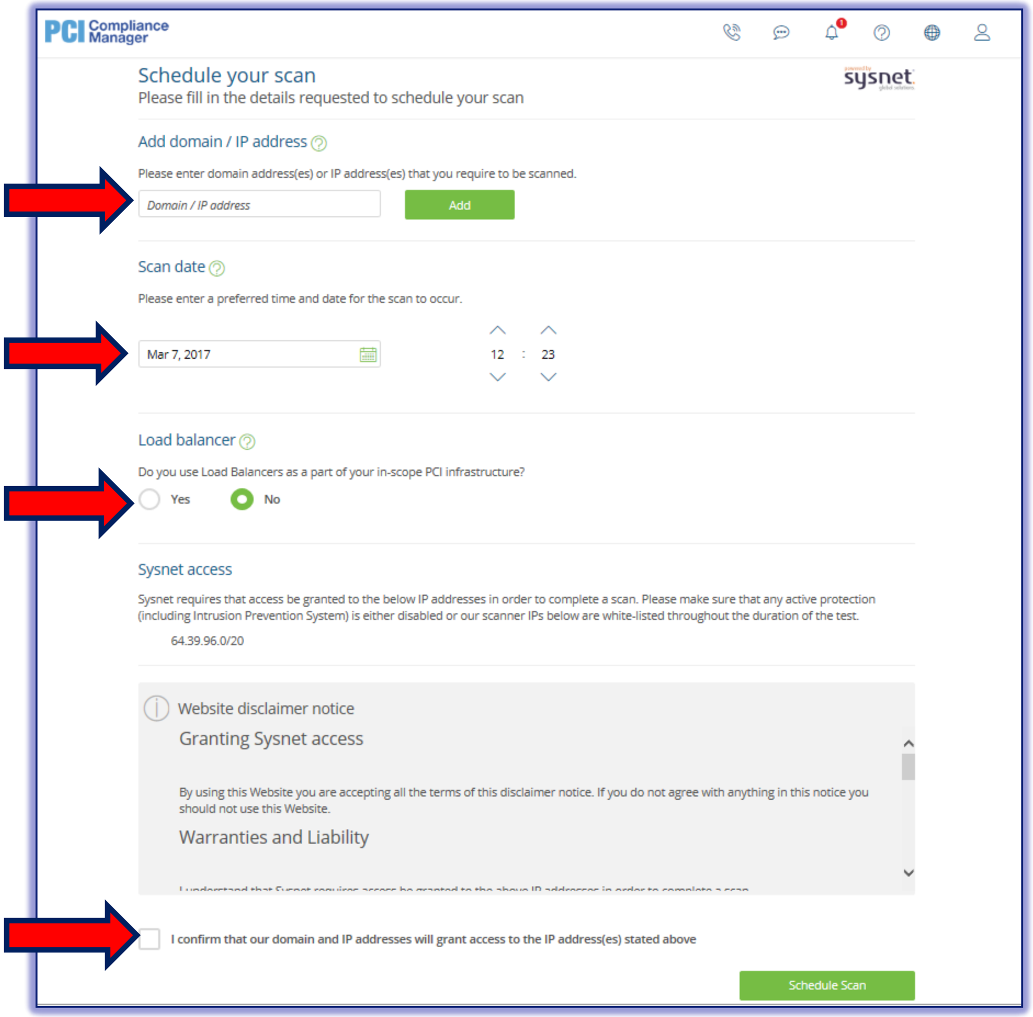
Manage multiple domains / IP addresses

Create a list of your domain names or your IP addresses that require scanning

Upload results

Upload your validated scan results from a 3rd party Approved Scanning Vendor (ASV)

Scheduling a Scan



Schedule your scan

Please fill in the details requested to schedule your scan

Add domain / IP address

Please enter domain address(es) or IP address(es) that you require to be scanned.

Scan date

Please enter a preferred time and date for the scan to occur.

Mar 7, 2017 12 : 23

Load balancer

Do you use Load Balancers as a part of your in-scope PCI infrastructure?

○ Yes ● No

Sysnet access

Sysnet requires that access be granted to the below IP addresses in order to complete a scan. Please make sure that any active protection (including Intrusion Prevention System) is either disabled or our scanner IPs below are white-listed throughout the duration of the test.

64.39.96.0/20

Website disclaimer notice

Granting Sysnet access

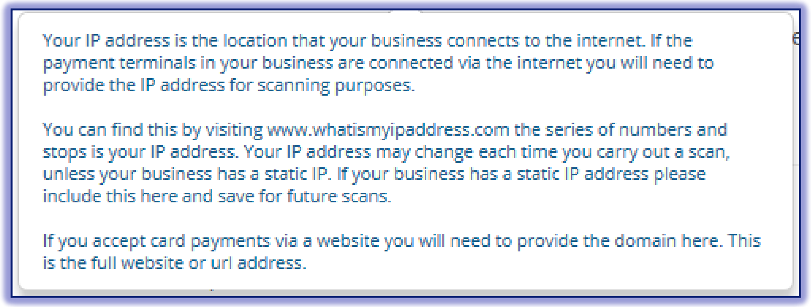
By using this Website you are accepting all the terms of this disclaimer notice. If you do not agree with anything in this notice you should not use this Website.

Warranties and Liability

I understand that Sysnet requires access be granted to the above IP addresses in order to complete a scan

□ I confirm that our domain and IP addresses will grant access to the IP address(es) stated above

Add domain/IP address help text

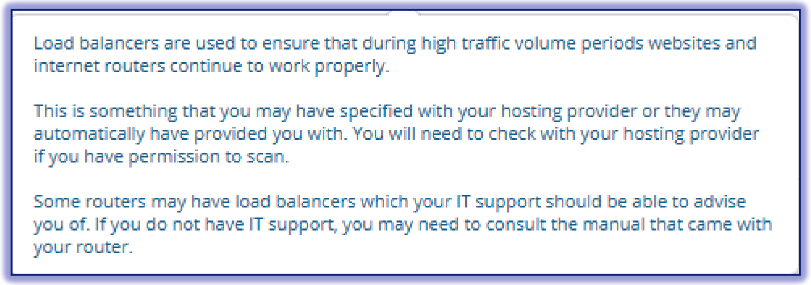


Your IP address is the location that your business connects to the internet. If the payment terminals in your business are connected via the internet you will need to provide the IP address for scanning purposes.

You can find this by visiting www.whatismyipaddress.com the series of numbers and stops is your IP address. Your IP address may change each time you carry out a scan, unless your business has a static IP. If your business has a static IP address please include this here and save for future scans.

If you accept card payments via a website you will need to provide the domain here. This is the full website or url address.

Load Balancer help text

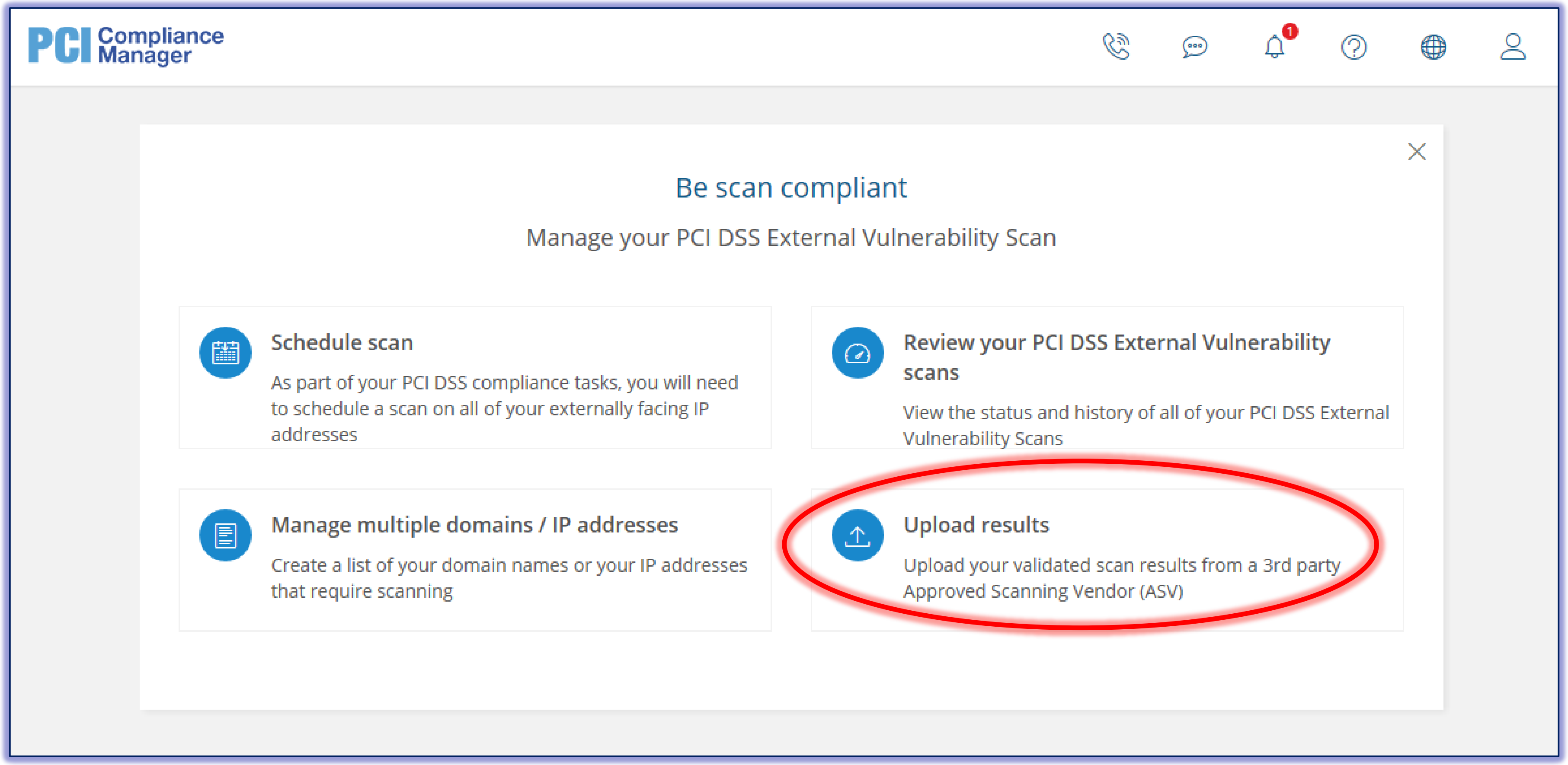


Load balancers are used to ensure that during high traffic volume periods websites and internet routers continue to work properly.

This is something that you may have specified with your hosting provider or they may automatically have provided you with. You will need to check with your hosting provider if you have permission to scan.

Some routers may have load balancers which your IT support should be able to advise you of. If you do not have IT support, you may need to consult the manual that came with your router.

Uploading a Scan



Be scan compliant

Manage your PCI DSS External Vulnerability Scan

Schedule scan

As part of your PCI DSS compliance tasks, you will need to schedule a scan on all of your externally facing IP addresses

Review your PCI DSS External Vulnerability scans

View the status and history of all of your PCI DSS External Vulnerability Scans

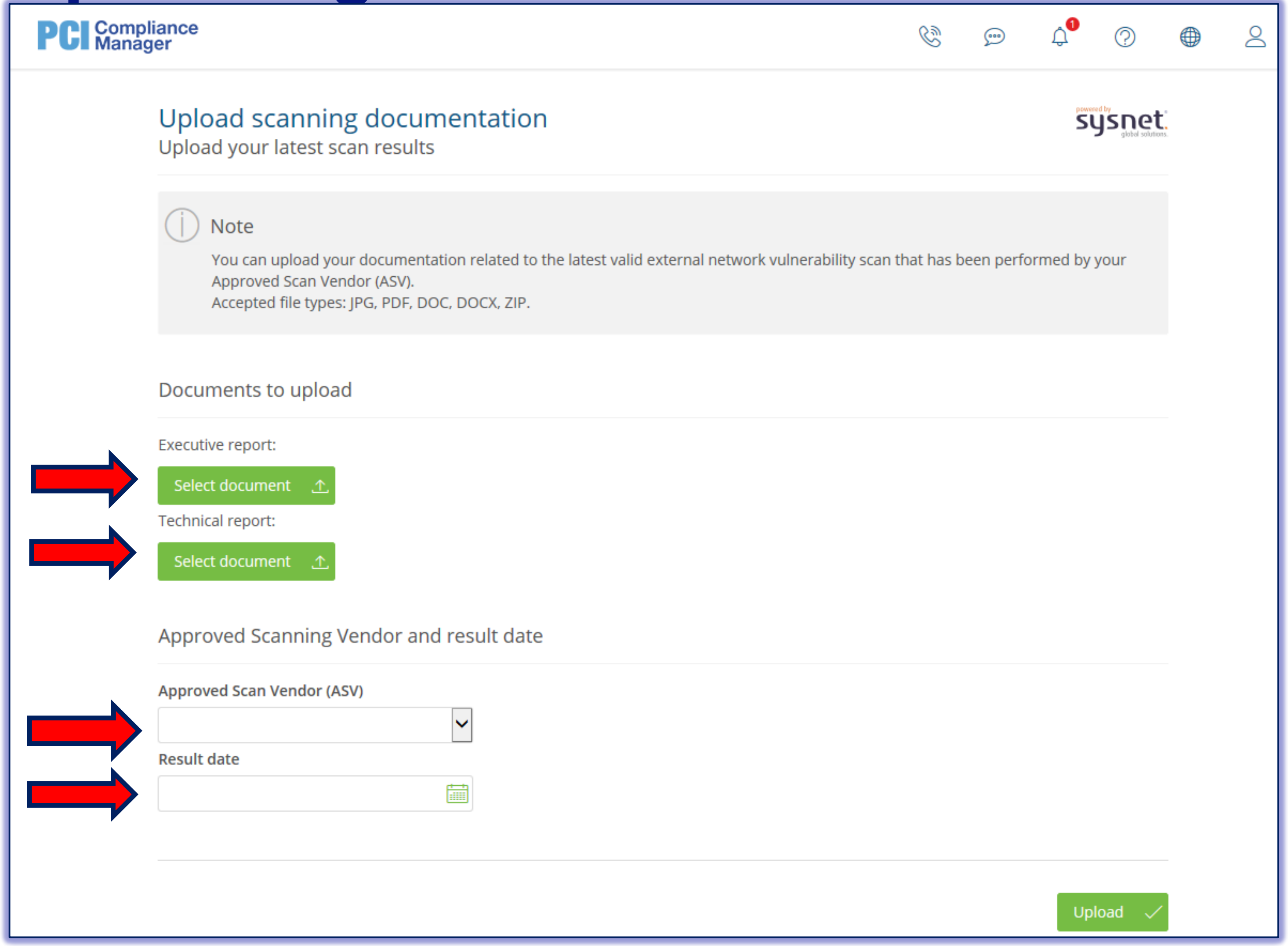
Manage multiple domains / IP addresses

Create a list of your domain names or your IP addresses that require scanning

Upload results

Upload your validated scan results from a 3rd party Approved Scanning Vendor (ASV)

Uploading a Scan



Upload scanning documentation

Upload your latest scan results

Note

You can upload your documentation related to the latest valid external network vulnerability scan that has been performed by your Approved Scan Vendor (ASV).
Accepted file types: JPG, PDF, DOC, DOCX, ZIP.

Documents to upload

Executive report:

Select document

Technical report:

Select document

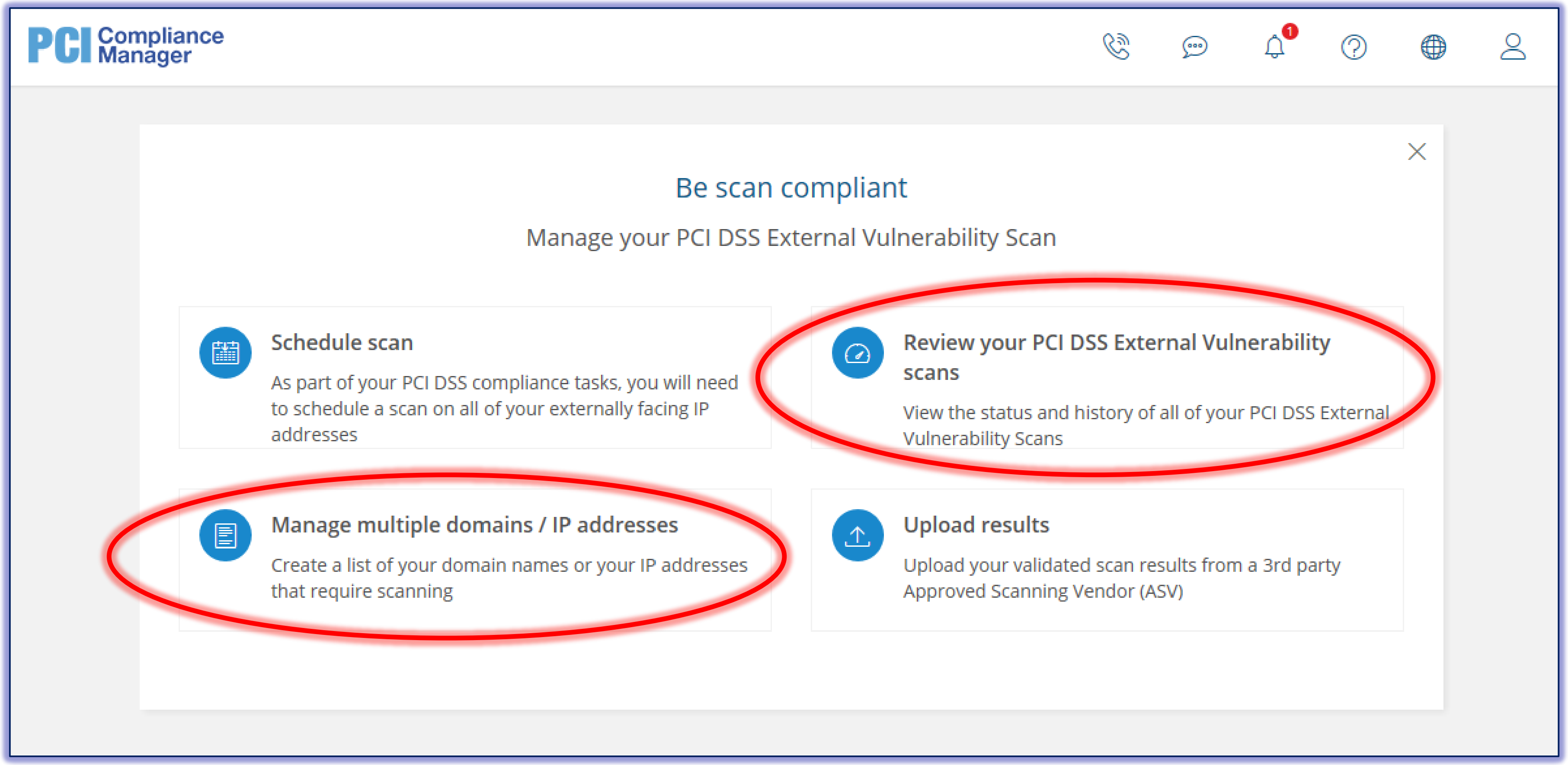
Approved Scanning Vendor and result date

Approved Scan Vendor (ASV)

Result date

Upload

Other Scan options



Be scan compliant

Manage your PCI DSS External Vulnerability Scan

Schedule scan

As part of your PCI DSS compliance tasks, you will need to schedule a scan on all of your externally facing IP addresses

Review your PCI DSS External Vulnerability scans

View the status and history of all of your PCI DSS External Vulnerability Scans

Manage multiple domains / IP addresses

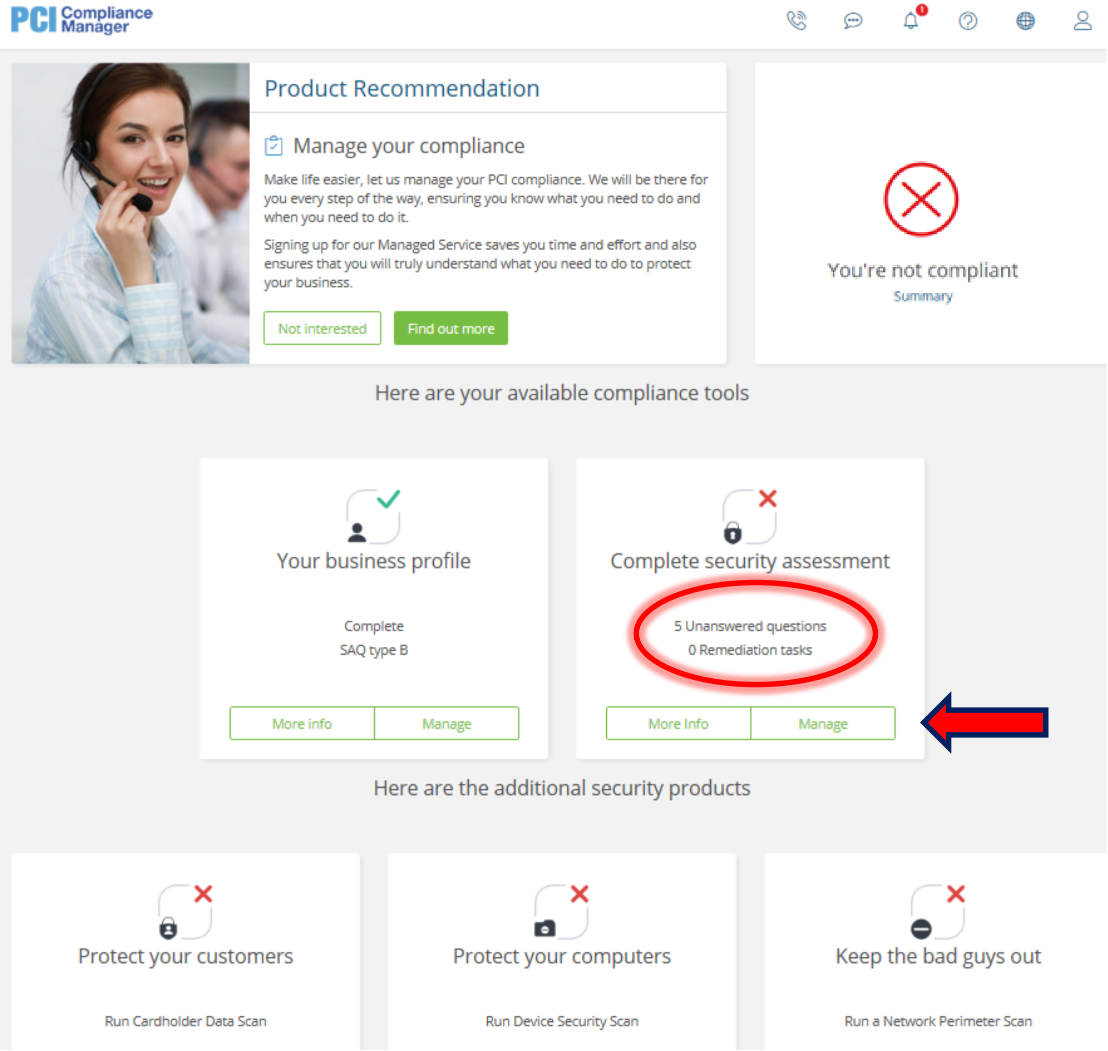
Create a list of your domain names or your IP addresses that require scanning

Upload results

Upload your validated scan results from a 3rd party Approved Scanning Vendor (ASV)

SAQ

Main Page



PCI Compliance Manager

Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

You're not compliant

Here are your available compliance tools

Your business profile

Complete
SAQ type B

Complete security assessment

5 Unanswered questions
0 Remediation tasks

Here are the additional security products

Protect your customers

Run Cardholder Data Scan

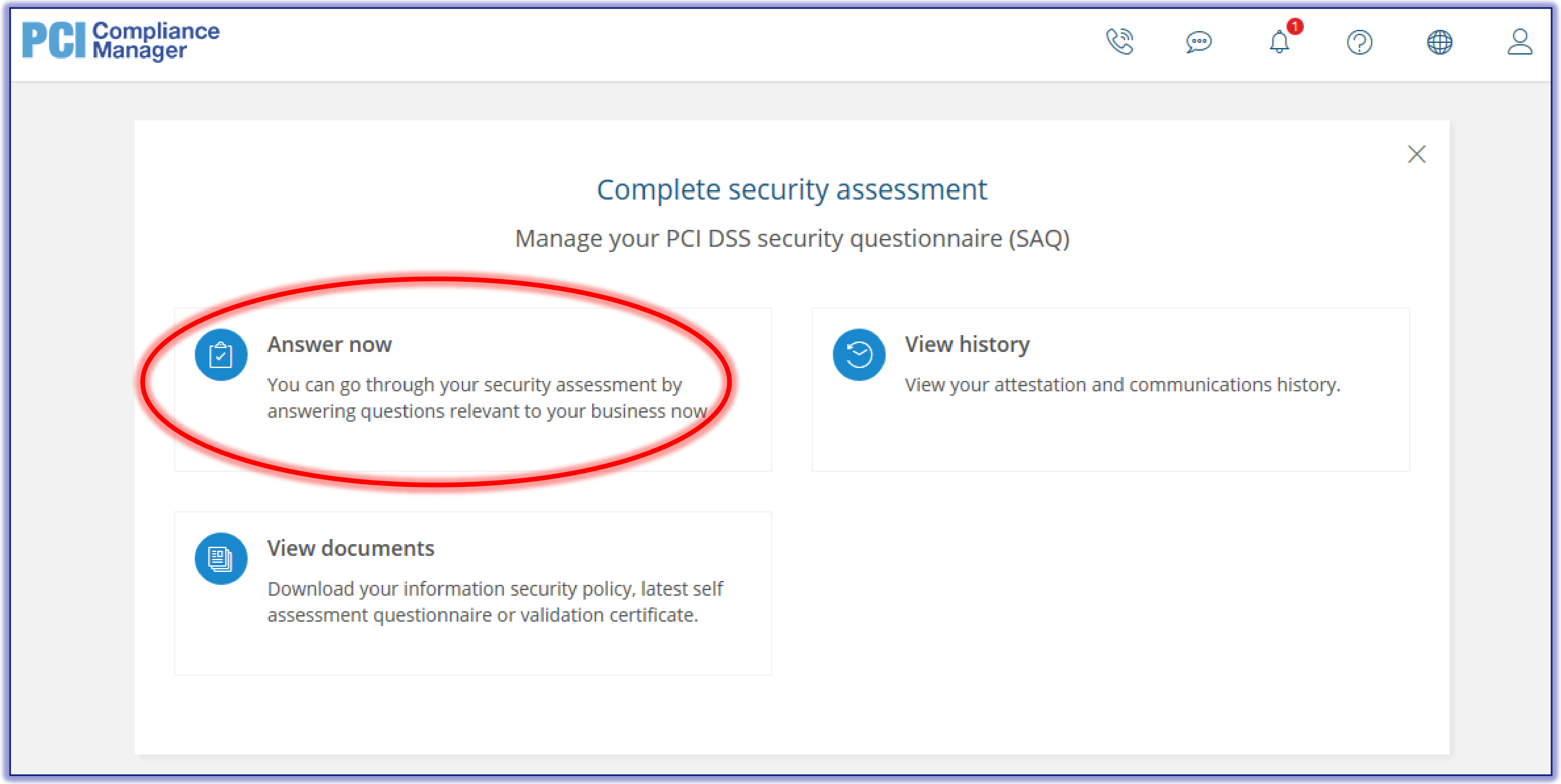
Protect your computers

Run Device Security Scan

Keep the bad guys out

Run a Network Perimeter Scan

Completing the SAQ



Complete security assessment

Manage your PCI DSS security questionnaire (SAQ)

Answer now

You can go through your security assessment by answering questions relevant to your business now

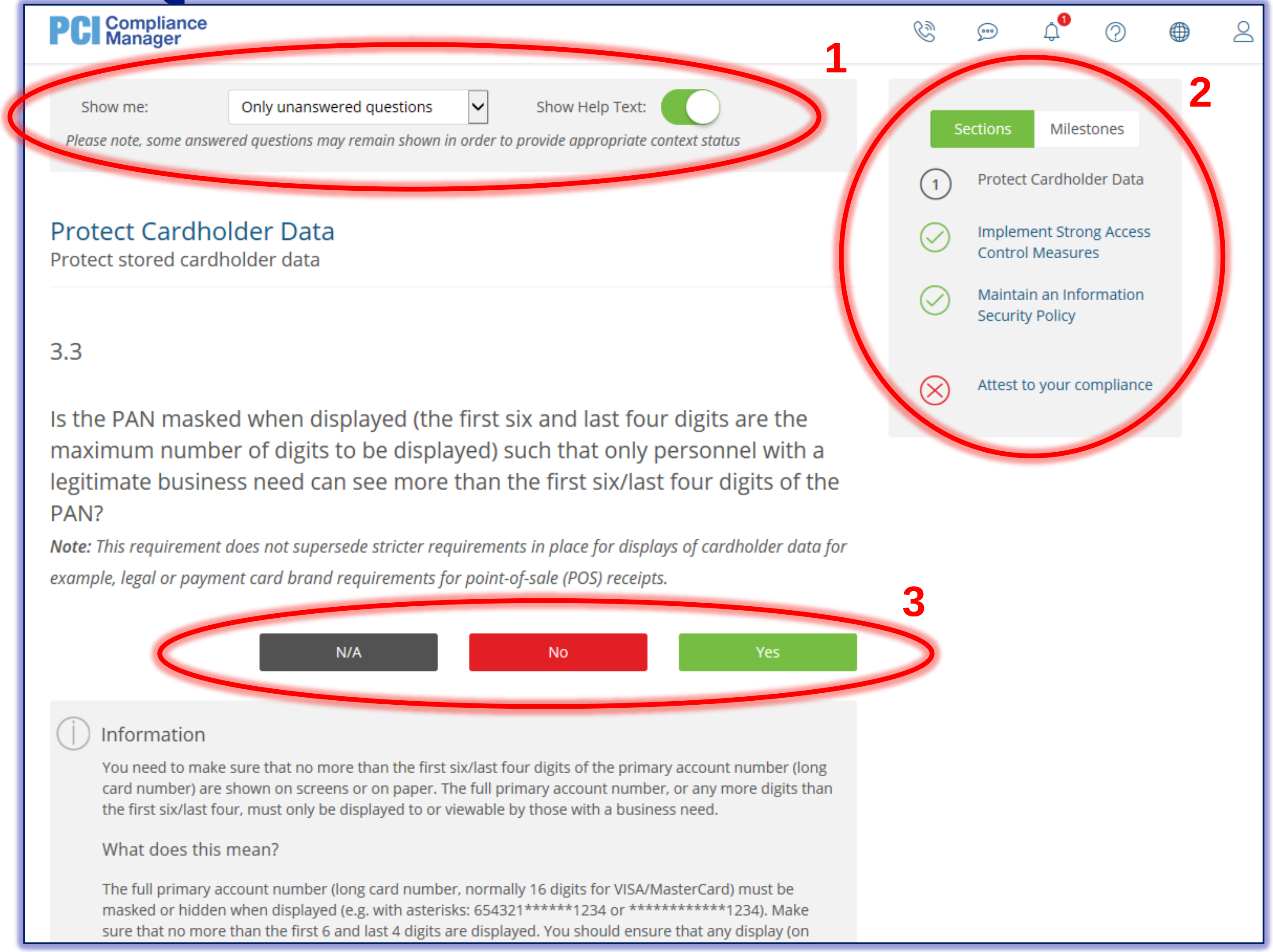
View history

View your attestation and communications history.

View documents

Download your information security policy, latest self assessment questionnaire or validation certificate.

SAQ



Show me: Only unanswered questions

Show Help Text:

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

1 Protect Cardholder Data

✓ Implement Strong Access Control Measures

✓ Maintain an Information Security Policy

⊗ Attest to your compliance

Protect Cardholder Data

Protect stored cardholder data

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.*

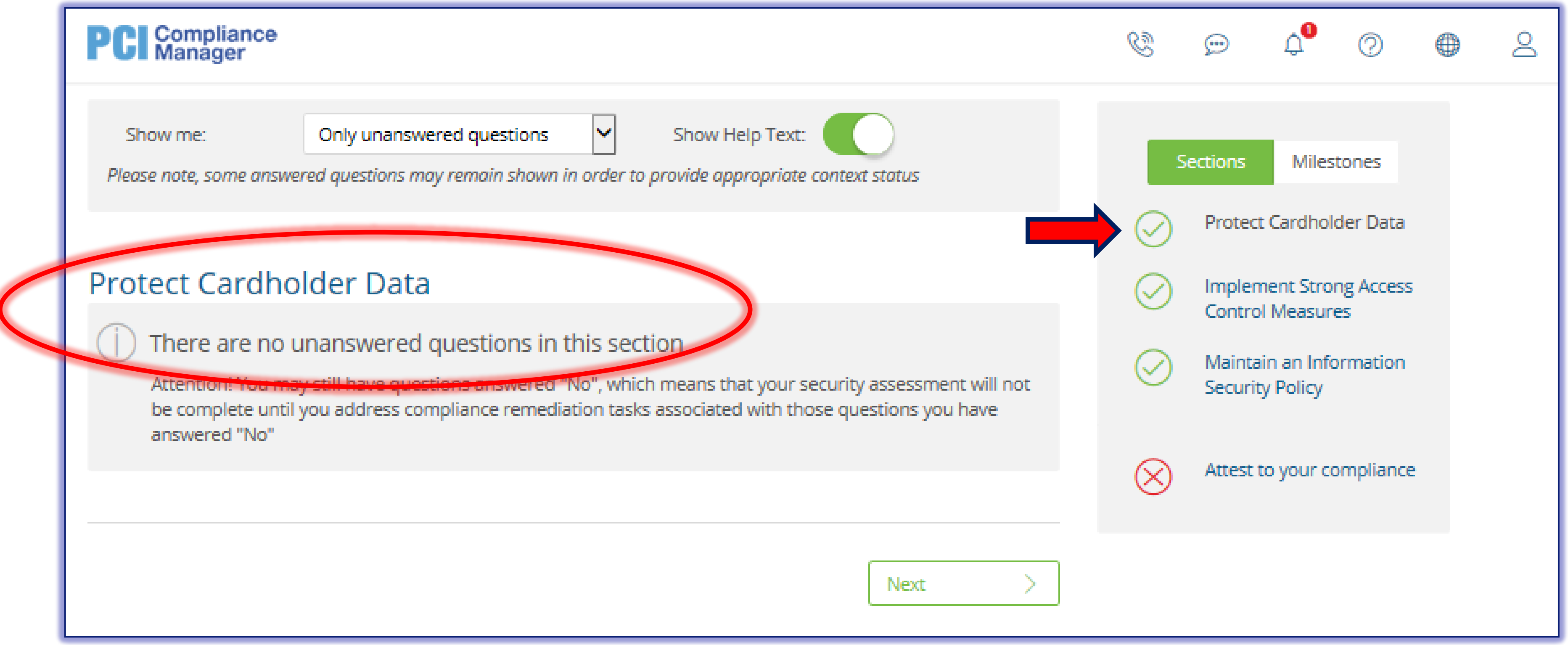
Information

You need to make sure that no more than the first six/last four digits of the primary account number (long card number) are shown on screens or on paper. The full primary account number, or any more digits than the first six/last four, must only be displayed to or viewable by those with a business need.

What does this mean?

The full primary account number (long card number, normally 16 digits for VISA/MasterCard) must be masked or hidden when displayed (e.g. with asterisks: 654321******1234 or ************1234). Make sure that no more than the first 6 and last 4 digits are displayed. You should ensure that any display (on

SAQ



Show me: Only unanswered questions Show Help Text:

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

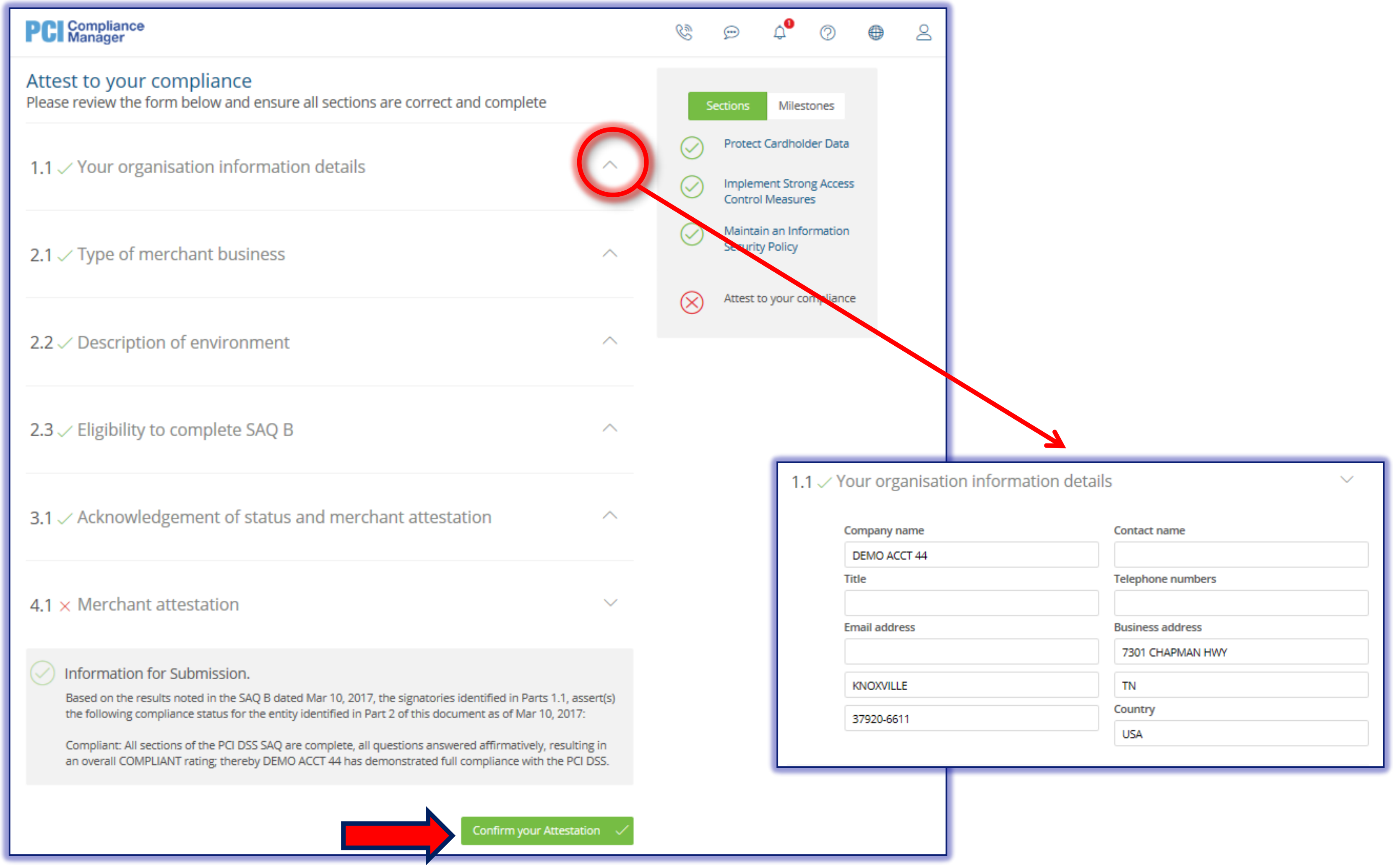
Protect Cardholder Data

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"

Next
Sections
Milestones
✓ Protect Cardholder Data
✓ Implement Strong Access Control Measures
✓ Maintain an Information Security Policy
☒ Attest to your compliance

Attesting



Attest to your compliance

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

- 1.1 ✓ Your organisation information details
- 2.1 ✓ Type of merchant business
- 2.2 ✓ Description of environment
- 2.3 ✓ Eligibility to complete SAQ B
- 3.1 ✓ Acknowledgement of status and merchant attestation
- 4.1 ✗ Merchant attestation

Information for Submission.

Based on the results noted in the SAQ B dated Mar 10, 2017, 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 Mar 10, 2017:

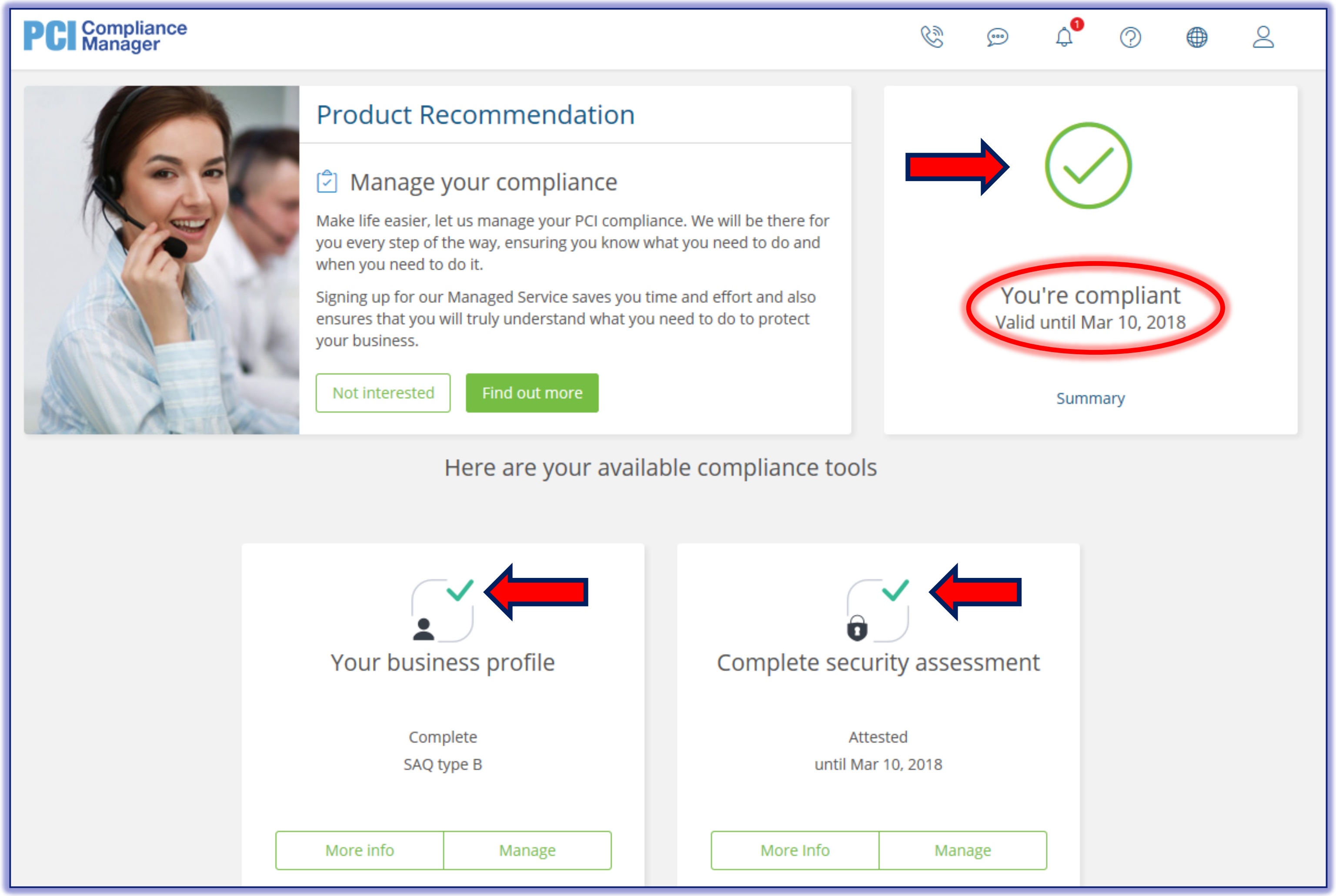
Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby DEMO ACCT 44 has demonstrated full compliance with the PCI DSS.

- ✓ Protect Cardholder Data
- ✓ Implement Strong Access Control Measures
- ✓ Maintain an Information Security Policy
- ✗ Attest to your compliance

1.1 ✓ Your organisation information details

Company name: DEMO ACCT 44	Contact name:
Title:	Telephone numbers:
Email address:	Business address: 7301 CHAPMAN HWY
KNOXVILLE	TN
37920-6611	Country: USA

Compliant



PCI Compliance Manager

Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

You're compliant
Valid until Mar 10, 2018

Here are your available compliance tools

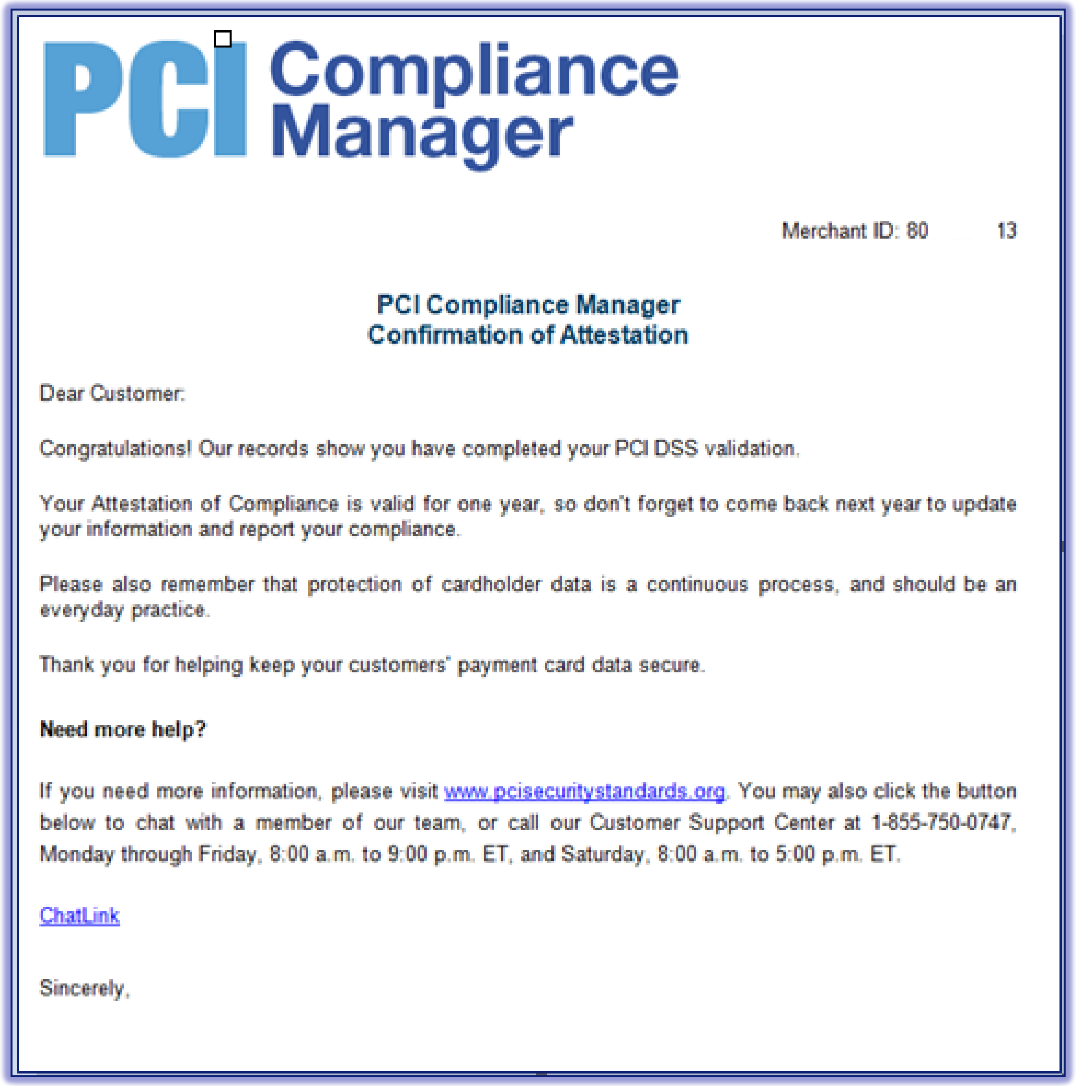
Your business profile

Complete
SAQ type B

Complete security assessment

Attested
until Mar 10, 2018

Compliant



PCI Compliance Manager

Merchant ID: 80 13

PCI Compliance Manager
Confirmation of Attestation

Dear Customer:

Congratulations! Our records show you have completed your PCI DSS validation.

Your Attestation of Compliance is valid for one year, so don't forget to come back next year to update your information and report your compliance.

Please also remember that protection of cardholder data is a continuous process, and should be an everyday practice.

Thank you for helping keep your customers' payment card data secure.

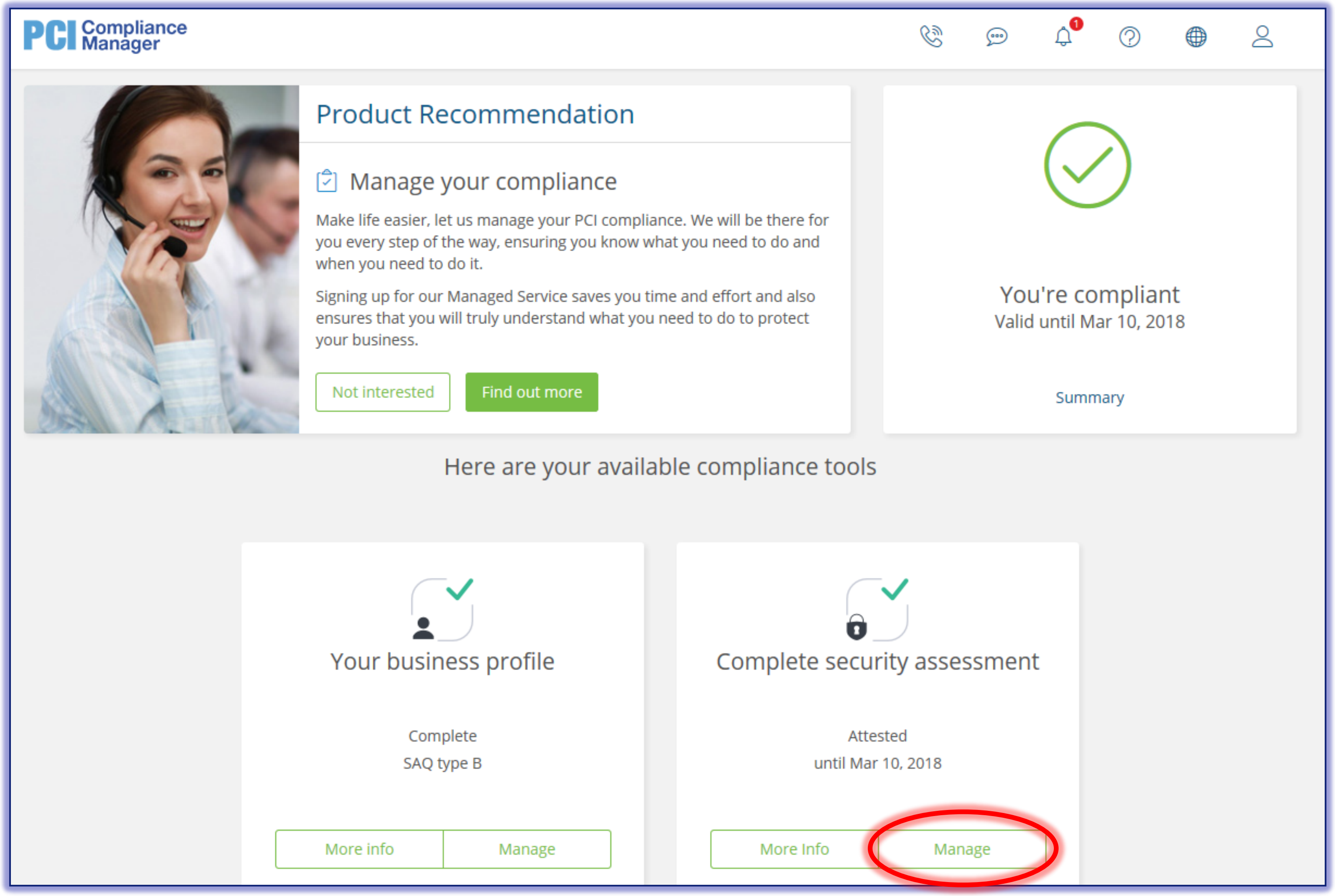
Need more help?

If you need more information, please visit www.pcisecuritystandards.org. You may also click the button below to chat with a member of our team, or call our Customer Support Center at 1-855-750-0747, Monday through Friday, 8:00 a.m. to 9:00 p.m. ET, and Saturday, 8:00 a.m. to 5:00 p.m. ET.

ChatLink

Sincerely,

Compliant



Product Recommendation

Manage your compliance

Make life easier, let us manage your PCI compliance. We will be there for you every step of the way, ensuring you know what you need to do and when you need to do it.

Signing up for our Managed Service saves you time and effort and also ensures that you will truly understand what you need to do to protect your business.

You're compliant
Valid until Mar 10, 2018

Here are your available compliance tools

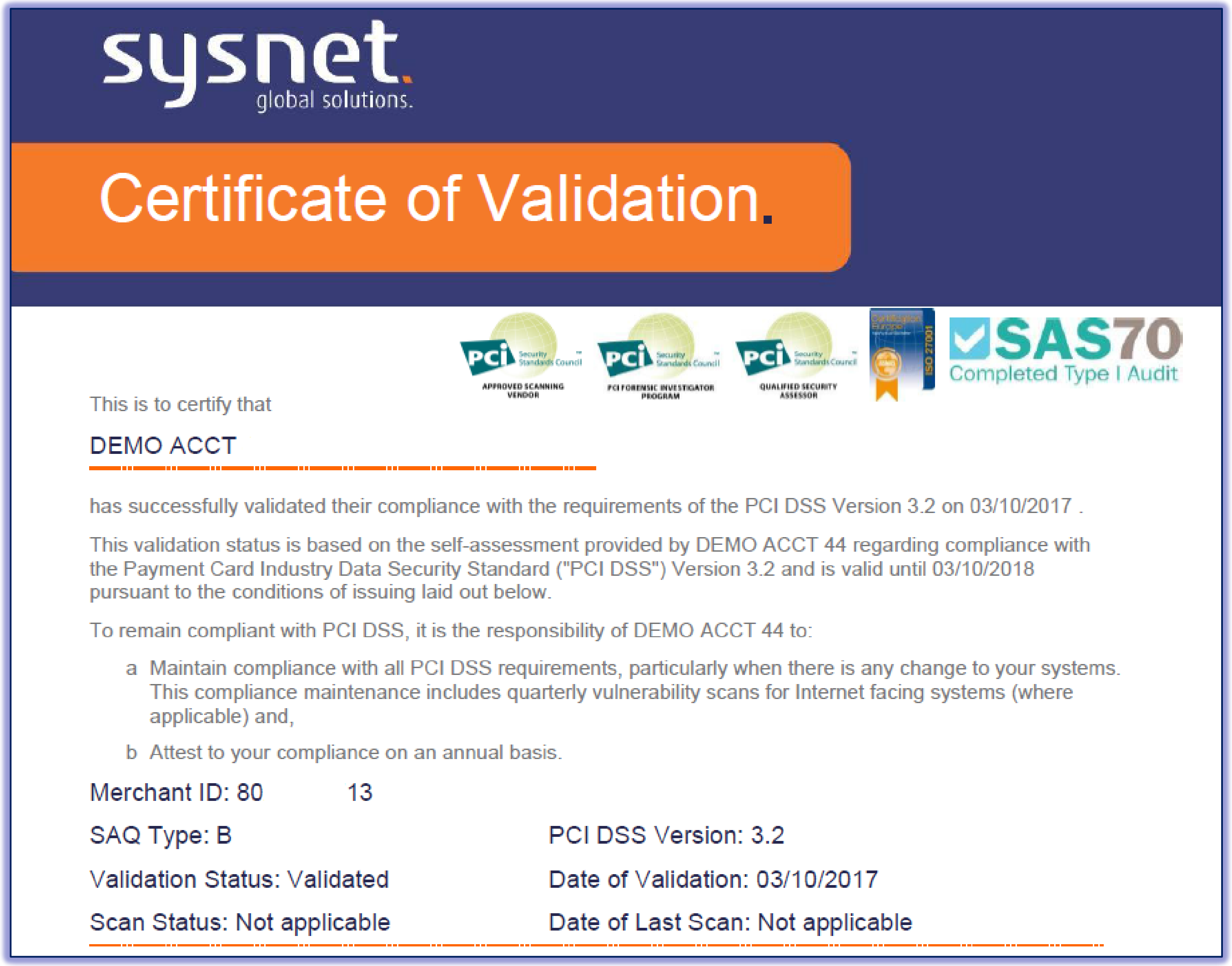
Your business profile

Complete
SAQ type B

Complete security assessment

Attested
until Mar 10, 2018

Certificate



sysnet global solutions.

Certificate of Validation.

PCI Security Standards Council APPROVED SCANNING VENDOR

PCI Security Standards Council PCI FORENSIC INVESTIGATOR PROGRAM

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

ISO 27001

SAS70 Completed Type I Audit

This is to certify that

DEMO ACCT

has successfully validated their compliance with the requirements of the PCI DSS Version 3.2 on 03/10/2017 .

This validation status is based on the self-assessment provided by DEMO ACCT 44 regarding compliance with the Payment Card Industry Data Security Standard ("PCI DSS") Version 3.2 and is valid until 03/10/2018 pursuant to the conditions of issuing laid out below.

To remain compliant with PCI DSS, it is the responsibility of DEMO ACCT 44 to:

a Maintain compliance with all PCI DSS requirements, particularly when there is any change to your systems. This compliance maintenance includes quarterly vulnerability scans for Internet facing systems (where applicable) and,

b Attest to your compliance on an annual basis.

Merchant ID: 80 13

SAQ Type: B	PCI DSS Version: 3.2
Validation Status: Validated	Date of Validation: 03/10/2017
Scan Status: Not applicable	Date of Last Scan: Not applicable