

Merchant User Guide



Updated April 2025

Merchant User Guide

What is the PCI DSS	3
Getting started – How it works	4
Getting started – How to access the online portal	5
Your starting dashboard	6
Your business profile	7
Your updated dashboard	8
Complete security assessment	11
Uploading a valid Attestation of Compliance	15
Be scan compliant – External Vulnerability Scanning	17
Validation complete – downloading your documents	20

What is PCI DSS

The PCI DSS is a set of security standards designed to protect your customers' credit card information. It is a checklist of things you need to do to keep your business safe from cyberattacks.

Businesses need to maintain PCI DSS compliance to protect their customers' credit card information from cyberattacks and data breaches. This helps prevent fraud, financial losses, and damage to the business's reputation.

The online portal will bring you through the relevant PCI DSS Self Assessment Questionnaire relevant to your business.

Our portal makes it easy for you to report and validate your compliance. It provides you with the tools you need to report on your security measures and ensure they meet the PCI DSS.

- PCI DSS compliance is an ongoing effort. You need to maintain strong security practices, train your staff, and work with your partners to protect your customers' card information.

VIKINGCLOUD™

We use strictly necessary cookies to enable core functionality of this site. We do not set any other cookies or similar technologies via this site. For more detailed information the strictly necessary cookies, please see our cookies policy. [COOKIES POLICY](#) [CLOSE](#)

Please login

MID/ Username*
Test

Password*
.....

LOGIN

[FORGOT PASSWORD](#) | [FORGOT USERNAME](#)

Welcome to your PCI DSS Programme

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 PCI DSS programme will help you to take the steps you need to comply with the PCI DSS standard and protect your business.

Getting Started – How it Works



Online chat support and phone support available if you get stuck.

GETTING STARTED

Access the online portal — once boarded: Your username and password instructions are sent to you via email.

3-4 STEP PROCESS

1

Your business profile

Series of simplified questions asking you how you accept card payments in your business.

2

Complete security assessment

Based on the answers from the business profile. You will then have to answer the SAQ questions.

3

Attestation of Compliance (AOC)

On completion of the relevant sections, you will be prompted to attest to your compliance. This generates your AOC.

4

Be scan compliant

You may need to scan either your internet connection, if using an internet connected terminal, or your website if capturing payments online. Passing scans are required every 90 days throughout the year.

THROUGHOUT THE YEAR

Ongoing throughout the year — Maintain Compliance

As a business accepting card payments, you need to maintain your compliance ongoing. If you have tasks such as ASV scanning, we'll notify you whenever they're due.

[GO TO CONTENTS >](#)

Getting started

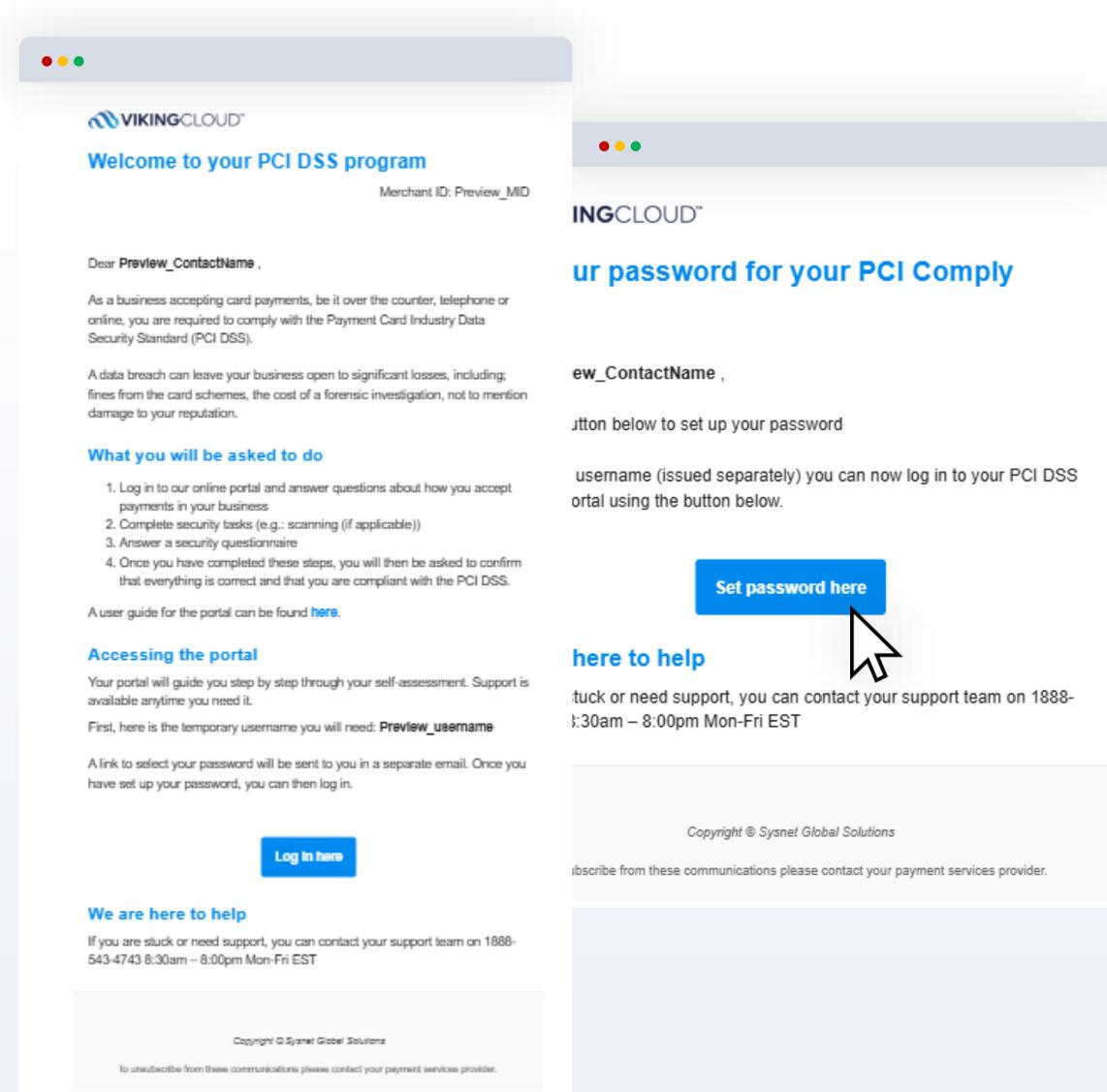
- How to access the online portal

Once your account has been set up on the PCI DSS portal, you will be sent two emails to access your account.

- The first email includes your username.
- The second will include instructions with a unique link to set up your password.

Once you have created your password, you can access the portal.

- When you log in to the portal for the first time, you will be prompted to update your account details, including username if you wish to. Check your spam or clutter folder for emails from notifications@complywithpci.com to ensure you continue to receive your program email notifications.



Your starting dashboard

Once logged in, you will land on your dashboard.

For first time users – you will need to provide information regarding how you accept card payments in your business to determine what assessment type you will have to complete to comply with the PCI DSS.

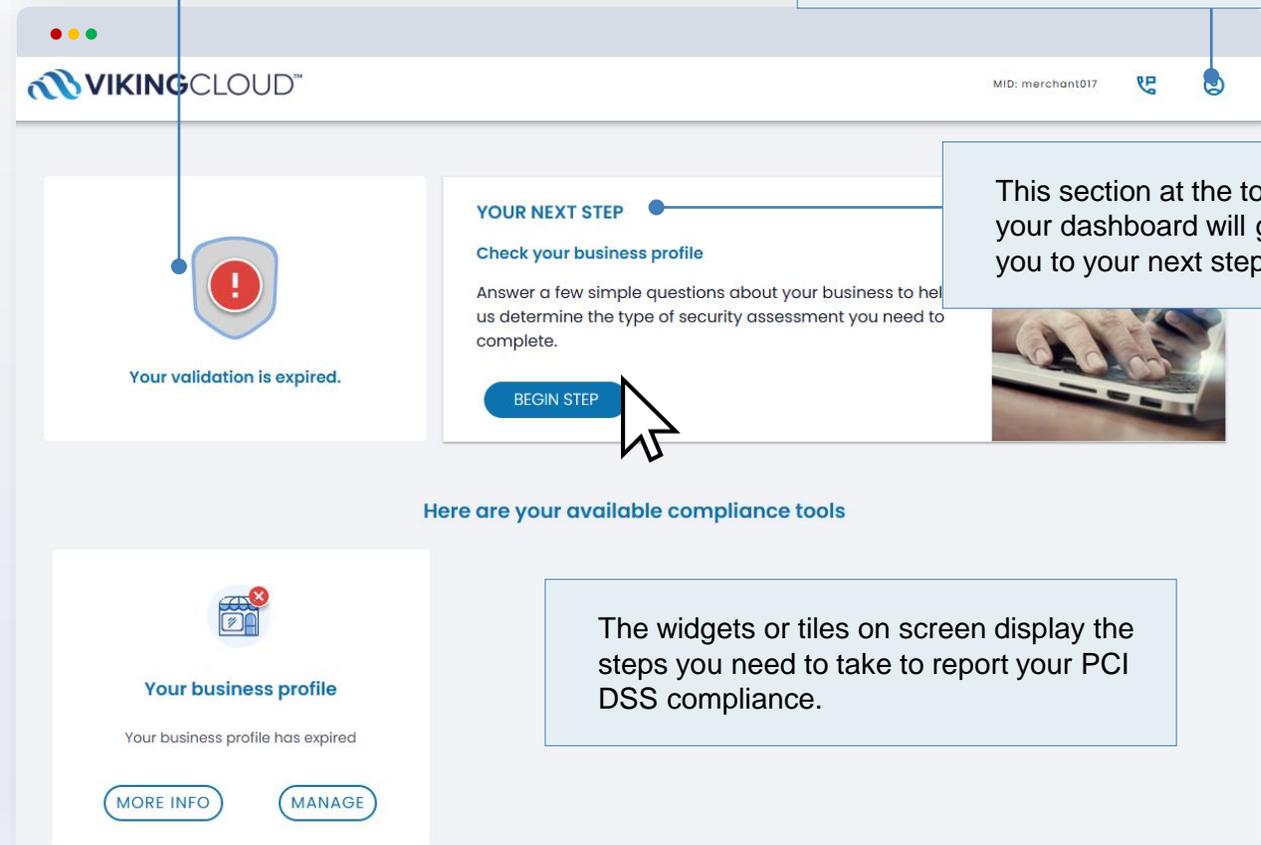
Simply click on the “**Manage**” button on “**Your business profile**” widget and follow the instructions.

Once this section is complete, you will see your additional compliance widgets and tools.

“**Your next step**” will direct you to your next task, simply select “**Begin step**” to continue.

Your compliance status is displayed here in the top left box.

Help options are available to you from the top right of the menu bar. You can also update your account details, add users and more from here.



This section at the top of your dashboard will guide you to your next step.

The widgets or tiles on screen display the steps you need to take to report your PCI DSS compliance.

Your business profile

– what you need to know:

You will be guided through a series of questions asking how you accept payments in your business. The questions will range from the technology you use, to methods by which you transfer or store data.

Select the options that apply to your business and use the “Next” button at the bottom right of the screen to move to the next question.

Make sure that you select all answers that apply to your business were applicable.

If you need further clarification, more information is available by clicking the help icon next to each question. You also have support on hand via the menu bar at the top of the screen.

If you have a currently valid Attestation of Compliance (AOC):

One of the first questions in your business profile will ask you if you recently validated your PCI compliance with another assessment company.

If you have a recently completed, still valid AOC, then you can select the option to upload your Attestation of Compliance to the portal. Page 15 of this guide gives you step by step upload instructions.

The image displays two screenshots of the VikingCloud merchant user interface. The top screenshot shows the 'Select Your Processing Method' screen, which asks the user to select all methods used for card payments. The options are: Payment Terminal (checked), Virtual Terminal, Integrated POS Terminal, and Pay by Link. The bottom screenshot shows the 'Payment Terminal' screen, which asks the user to indicate how the terminal connects to the payment processor. The options are: Phone line (checked), Internet, and Cellular wireless. Both screens feature a 'PREVIOUS' button on the left and a 'NEXT' button on the right.

Your business profile

Information Security Policy

As part of maintaining your PCI DSS compliance – it is mandatory that you have an Information Security Policy.

- This document sets out the procedures you need to follow to handle customer cardholder information securely.

You will be asked if you have an Information Security Policy and if not, you can download the template provided by clicking “Download”.

Once downloaded you must review it and update it as follows:

1. Tailor the sample template so that it reflects how you accept card payments and handle cardholder data in your business.
2. Ensure that all staff and any third parties in your business read, sign and date your document. This will ensure that you have a record and confirmation that they understand what is expected of them.
3. Finally - you must always keep your Information Security Policy on your business’ premises, and if anything changes in how you accept card payments, you will need to update your policy to reflect the changes.

VIKINGCLOUD™ MID: merchant017

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.

[PREVIOUS](#) [NEXT](#)

You can download your Information Security Policy template from the 'Download' link in this question. By answering this question 'Yes' you have confirmed that you are committing to implementing all of the provisions contained in the document template as they apply to your organization.

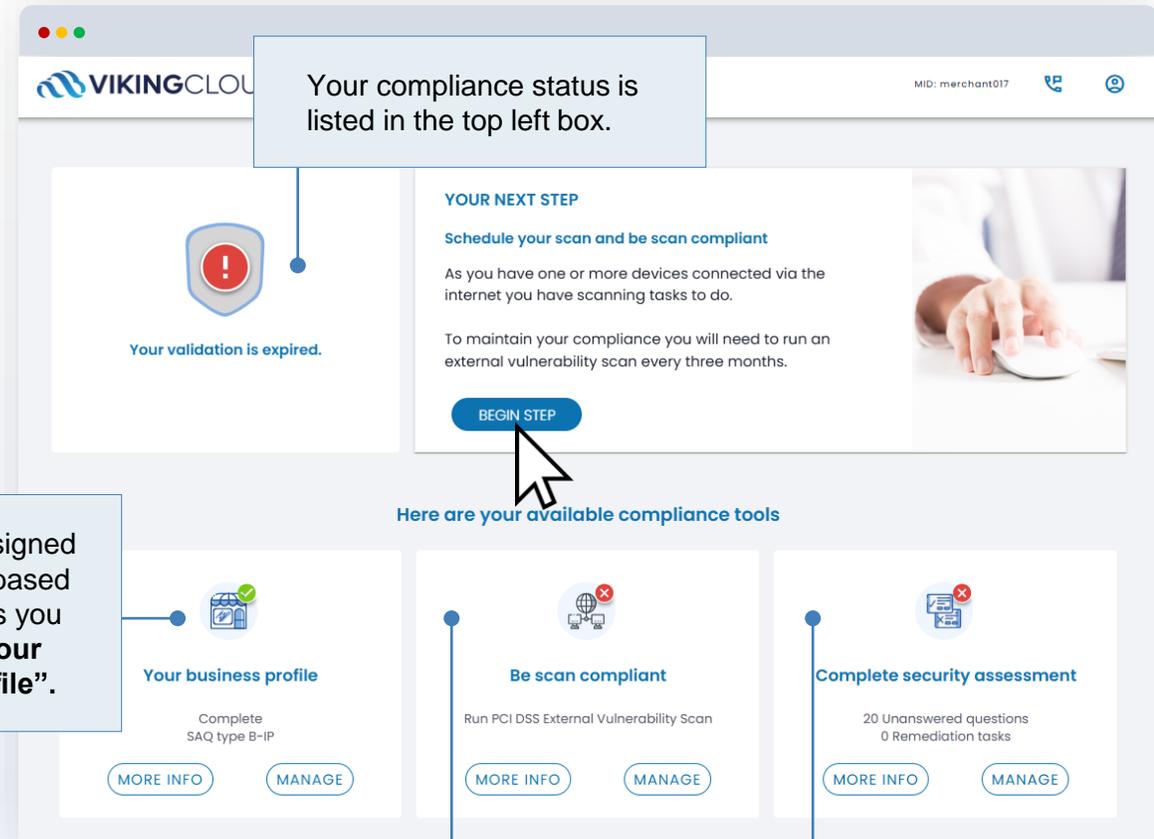
[CLOSE](#)

Your updated dashboard

Once you have answered your profile questions, you will see your additional compliance widgets and tools.

Each widget has two buttons - a **“More Info”** button, for more information and a **“Manage”** button which you can select to complete your compliance tasks.

- All compliance tools presented to you for completion are based on the answers you provided in **“Your business profile”**.
- The **“Complete security assessment”** section will be visible to all businesses.
- The **“Be scan compliant”** displayed here will only be visible to those businesses who must complete external vulnerability scanning for compliance every 90days.



You will be assigned an SAQ type, based on the answers you provided in **“Your business profile”**.

If scanning applies to your business (based on your SAQ type, you can complete your scanning from the **“Be scan compliant”** widget. Click **‘Manage’** on the scan widget to begin.

Your remaining PCI requirements and attestation steps are available for completion via the **“Complete security assessment”** widget. To complete, simply click on **‘Manage’**.

Complete security assessment

– (Self-Assessment Questionnaire section)

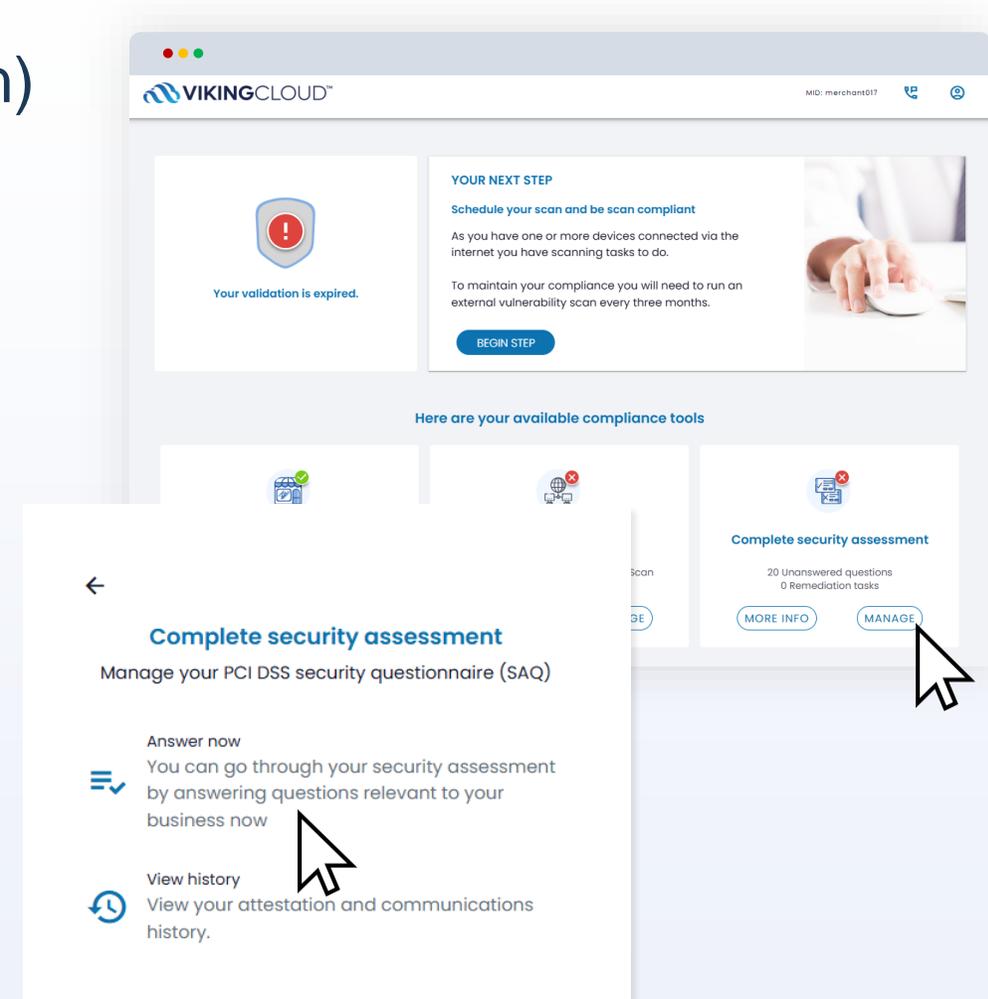
Your remaining PCI DSS Payment Card Industry Data Security Standard (PCI DSS) requirements and attestation steps are available for completion via the **“Complete security assessment”** widget.

You can select **“Manage”** to complete this section.

To note: A PCI DSS SAQ requirement is a specific security rule that you must follow to protect your customers credit card information.

This section uses the official language of the PCI DSS which can be technical at times. Each requirement includes help text and guidance to explain in detail how and where they apply.

You also have access to additional help and support from the top right on the menu bar.



Complete security assessment

– (Self-Assessment Questionnaire section - (SAQ))

At the top, from the dropdown you can select to view only your remaining unanswered questions, or all questions that apply – including prepopulated answers.

You can also hide or display the help text for each requirement, depending on your preference.

You will need to work your way through the remaining questionnaire by answering “Yes”, “No” or “N/A” to the questions.

The screenshot shows the VikingCloud interface for a security assessment. At the top, there is a dropdown menu labeled 'Show me:' with the option 'Only unanswered questions' selected. To the right of the dropdown is a 'Show Help Text:' section with 'Yes' and 'No' buttons. Below this is a disclaimer: 'Disclaimer: The English version, as available on the PCI SSC website, for all purposes, is considered the official version and, to the extent there are ambiguities or inconsistencies between the wording of this text and the English text, the English version will prevail.' The main section is titled 'Build and Maintain a Secure Network and Systems' with a requirement ID '1.2.5'. The text reads: 'All services, protocols and ports allowed are identified, approved, and have a defined business need.' Below this are three buttons: 'N/A', 'NO', and 'YES'. A note says 'OR Click here if you have a compensating control'. A 'Help answering this requirement' panel is open, showing 'Expected Testing' (Examine documentation, Examine configuration settings) and 'Information' (Purpose, Good Practice). The 'Purpose' section states: 'NSC Compromises often happen due to unused or insecure services (for example, telnet and FTP), protocols, and ports, since these can lead to unnecessary points of access being opened into the CDE. Additionally, services, protocols, and ports that are enabled but not in use are often overlooked and left unsecured and unpatched. By identifying the services, protocols, and ports necessary for business, entities can ensure that all other services, protocols, and ports are disabled or removed.' The 'Good Practice' section states: 'The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.'

Sections

The Sections panel on the right side of the screen displays your progress through the questionnaire.

Many of the questions may have been prepopulated for you based on your answers in the profile section.

The number displayed against each section indicates how many requirements you have left in each section.

If you see a check mark that means that section has been completed.

You can click on each section to navigate around and view the PCI DSS requirements in full.

Complete security assessment – (Self-Assessment Questionnaire section - (SAQ))

If there are requirements you cannot confirm you have in place, you will be asked to provide further explanation, and you may need to create a remediation task for yourself.

- You must fill out your reasons for non-compliance, the remediation action you intend to take and can then set a reminder to yourself to follow up.

You can continue with your remaining assessment questions. However, until these tasks are completed correctly you may not be able to confirm and attest that you are compliant with the PCI DSS.

It may also happen that a specific requirement does not apply to your business, if that is the case, you can select “**N/A**”. You will then need to provide information as to why it doesn’t apply and then continue to the next question.

Build and Maintain a Secure Network and Systems

1.2.5

All services, protocols and ports allowed are identified, approved, and have a defined business need.

OR [Click here if you have a compensating control](#)

You selected no

Reason for non-compliance*
0 / 1500

Complete documentation*
0 / 1500

Target date:* You will receive a email

Build and Maintain a Secure Network and Systems

1.2.5

All services, protocols and ports allowed are identified, approved, and have a defined business need.

OR [Click here if you have a compensating control](#)

You selected not applicable

Reason for this response*
0 / 1500

Complete security assessment – Attestation

Once you have answered all sections and requirements, the next step is for you to attest to your compliance.

This simply means to confirm and attest that the information you have provided is correct.

To review each of your sections and answers you can simply click to expand each menu.

Once satisfied that everything is present and correct, simply, select **“Confirm your Attestation”** at the bottom of the screen.

If you have external vulnerability scanning for compliance, then you will need to ensure that you have a passing scan and run your external scans at a minimum every 90days.

VIKINGCLOUD™

confirm your compliance

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

✓ Your organization information details

Company name merchant017 Contact name* contactmerchant017

Title Telephone numbers

Email address test17@sysnet.ie Business address 17 Main Street

Address Line 2 17 Main Street 2 Address Line 3 17 Main Street 3

Address Line 4 17 Main Street 4 Address Line 5 17 Main Street 5

Country Ireland

✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ B-IP

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

X Attestation

✓ Information for Submission.

Based on the results noted in the SAQ B-IP dated Apr 7, 2025, the signatories identified in Parts 11, osant(3) the following compliance status for the entity identified in Part 2 of this document as of Apr 7, 2025:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively. You are required to maintain compliance with PCI DSS at all times.

CONFIRM YOUR ATTESTATION

PREVIOUS

Sections

- ✓ Build and Maintain a Secure Network and Systems
- ✓ Protect Account Data
- ✓ Maintain a Vulnerability Management Program
- ✓ Implement Strong Access Control Measures
- ✓ Regularly Monitor and Test Networks
- ✓ Maintain an Information Security Policy
- ✓ Appendix A: Additional PCI DSS Requirements
- X Confirm your compliance

Uploading a valid Attestation of Compliance

If you wish to upload a currently valid Attestation of Compliance that you have completed elsewhere, you can do so via “**Your business profile**” widget.

1. You will be asked to choose your assessment method, choose “**Upload**”.
2. Next, you will need to select your current valid PCI DSS compliance assessment type, which you will find on the AOC that you are uploading. Choose the SAQ type and click “**Next**” and continue through the remaining profile questions.
3. Once you have completed the questions, you will be brought back to your dashboard where you will need to select “**Begin step**” to start the process for uploading your Attestation of Compliance (AoC).

The image shows two screenshots of the VikingCloud dashboard. The top screenshot displays the 'Choose an assessment method' section with two radio button options: 'Guide Me' and 'Upload'. The 'Upload' option is selected, and a mouse cursor is pointing at it. Below this is a 'PREVIOUS' button. To the right, a modal titled 'Your current valid PCI compliance type' is open, showing a list of SAQ types: SAQ A, SAQ A-EP, SAQ P2PE, SAQ B, and SAQ B-IP. The bottom screenshot shows the dashboard after the assessment method is chosen. A 'Your validation is expired' warning is visible. A 'YOUR NEXT STEP' section prompts the user to 'Confirm you're compliant' and upload their AoC, with a 'BEGIN STEP' button highlighted by a mouse cursor. Below this, there are two main dashboard widgets: 'Your business profile' (Complete SAQ type B) and 'Attestation' (Attestation upload). The 'Attestation' widget has 'ATTEST' and 'VIEW HISTORY' buttons.

Uploading a valid Attestation of Compliance

Once presented with your Attestation of Compliance upload screen.

1. Select **“Upload”**
 1. Click **“Select File”** this will open the file explorer on your device. Select the necessary document(s).
 2. Once uploaded you will need to confirm the document type, validation date, PCI DSS version, status and its completion status.
2. Review and confirm your eligibility in completing the SAQ type you have uploaded.
3. Confirm the validation effective date & PCI DSS version.
4. Check the boxes to acknowledge the conditions in relation to your status and attestation. Click **“Attest”** to finish. Your validation is now complete.

VIKINGCLOUD™ MID: merchant017

Attestation of compliance

i Attestation Requirements

In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document

Please **SELECT** or **UPLOAD** documents

Eligibility to complete SAQ B

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

- ✓ The merchant uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line the merchant processor) to take customers' payment card information.
- ✓ The standalone, dial-out terminals are not connected to any other systems within the merchant environment.
- ✓ The standalone, dial-out terminals are not connected to the Internet.
- ✓ The merchant does not store account data in electronic format.
- ✓ Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Assessment type **B** Validation effective date* PCI DSS Version*

Acknowledgement of status and attestation

- PCI DSS Self-Assessment Questionnaire B was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
- PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

ATTEST

Be scan compliant

– External Vulnerability Scanning

From your dashboard, select **“Manage”** on the **“Be scan compliant”** widget to view the scan management screen.

Or your **“Your next step”** will direct you to your scan management screen by simply selecting **“Begin step”** to continue.

To manage and run your scans, select the **“Schedule a scan”** option.

This will direct you to your main scan dashboard. You will be able to scan either your network IP, or your website, or both, depending on how you take payments in your business.

The image shows a screenshot of the VikingCloud dashboard. At the top, there's a navigation bar with the VikingCloud logo and user information (MID: merchant017). The main content area features several widgets. A prominent widget on the left has a red exclamation mark icon and the text "Your validation is expired." To its right, a "YOUR NEXT STEP" section titled "Schedule your scan and be scan compliant" explains that users need to run an external vulnerability scan every three months and includes a "BEGIN STEP" button. Below these are two more widgets: "Your business profile" (Complete SAQ type B-IP) and "Be scan compliant" (Run PCI DSS External Vulnerability Scan), both with "MORE INFO" and "MANAGE" buttons. A mouse cursor is pointing at the "BEGIN STEP" button. To the right, a separate window titled "Be scan compliant" shows a list of management options: "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), and "Upload results" (Upload your validated scan results from a 3rd party Approved Scanning Vendor (ASV)). A mouse cursor is also pointing at the "Schedule scan" option.

Be scan compliant

– External Vulnerability Scanning

If you take face to face payments using an internet connection, you will need to provide your network IP address. This must be the IP address used by your card payment machine. Instructions on how to find this is provided on the next page.

If you take payments via a website, you will need to scan your website payment pages. If unsure exactly what pages to scan, we recommend speaking to your web developer to identify the correct domain(s) to scan. You will be asked to confirm if you use a load balancer on your website.

“Scan date”: We recommend setting this to the current time and date for the scan to enter the queue.

“Load balancer”: This can be likened to a person in charge of your network directing the traffic, it is typically used for networks and websites with high traffic volumes.

More information on all these items is available via the help icons. Help is also available via chat as well as the help icons from the top menu bar.

Once you have completed all sections, select **“Schedule scan”** and the scan will be queued to run, it can take up to 48 hours to complete. You will receive an email when the scan is complete instructing you to log in and review the results.

- If you have a passing scan, you will need to confirm the results, once happy with the result, you can and must attest to the results of the scan for it to be recorded as a compliant scan.
- If you have remediation activities or a failing scan, you will need to follow the instructions and take any steps to improve the security of your environment. You may need to rerun the scan until you achieve a passing scan that you can attest to - which is necessary for maintaining your PCI DSS compliance.

What would you like to scan?

Domain: Schedule group scan

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

Domain / IP address* Add

Scan date

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

Scan date: April 7, 2025 Time: 10:48

Load Balancer?

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

Yes No

Sysnet access

In order to run the scan, we need you to grant access to the IP addresses listed below.

If you use security software such as a firewall in your organisation, you may need to white-list the below addresses in order for the scan to run successfully. Otherwise, you may block access to the scan, meaning it will fail. This will result in you being unable to successfully report your compliance.

If you are unsure how to do this, consult the help section of your firewall or contact your internet service provider for assistance.

What is an IP address?

An IP address is a series of numbers and dots that is your address on the internet. We need the correct address for your internet connection, to allow us to scan the correct connection - otherwise, we may scan someone else's network.

Dynamic IP addresses

Some internet service providers will assign you a "dynamic" IP address. This is an IP address that changes every time you connect and disconnect your internet router.

If you have a dynamic IP address, you need to update us with this new number every time you run your scan. This allows us to scan the correct connection.

If you are unsure as to whether you have a dynamic IP address, please contact your internet service provider who will be able to advise you. If you do have a dynamic IP, it's advisable to refrain from scheduling scans in advance, as your IP address may have changed by the time the scheduled scan runs.

- 64.59.96.0/20
- 154.59.121.0/24
- 139.87.104.123/32
- 139.87.117.66/32
- 139.87.112.0/29
- 143.144.198.156/32
- 156.105.209.126/32

Website disclaimer notice

Granting Sysnet access

By using this Website you are accepting all of 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 will ensure that any active protection (including Intrusion Prevention System) is disabled or that I will white-listed Sysnet's above IPs for the duration of the test.

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

In no event will Sysnet be liable for any incidental, indirect, consequential or special damages of any kind, or any damages whatsoever, including, without limitation, those resulting from loss of profit, loss of contracts, goodwill, data, information, income, anticipated savings or business relationships, whether or not advised of the possibility of such damage, arising out of or in connection with the use of this website or any linked websites. In addition, Sysnet shall not be liable for any fees, charges, costs or penalties imposed by any third party vendors used by you or any other person on your behalf (including but not limited to any internet or other service provider or other third party) in connection with, on foot of, or a result of your use of this website or the services contained therein.

Exceptions

Nothing in this disclaimer notice excludes or limits any warranty implied by law for death, fraud, personal injury through negligence, or anything else which it would not be lawful for Sysnet to exclude.

License to use this Website

By using this website you agree to the exclusions and limitations of liability stated above and accept them as reasonable. Do not use this website if you do not agree that they are reasonable. If any of the points in this disclaimer notice are found to be unenforceable under applicable law that will have no bearing on the enforceability of the rest of the disclaimer notice. Material on this website, including text and images, is protected by copyright law and is copyright to Sysnet unless credited otherwise. It may not be copied, reproduced, republished, downloaded, posted, broadcast or transmitted in any way except for your own personal, non-commercial use. Prior written consent of the copyright holder must be obtained for any other use of material. Copyright of the images on this site shall remain with the copyright owner at all times. No part of this site may be distributed or copied for any commercial purpose or financial gain. All intellectual property rights in relation to this website are reserved and owned by Sysnet.

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

SCHEDULE SCAN

Be scan compliant

– External Vulnerability Scanning

How to find your IP Address if you take face to face payments and use an internet connection

Your IP address is a series of numbers and dots that is your address on the internet. This helps to ensure the scan runs on the correct network. To find your IP address:

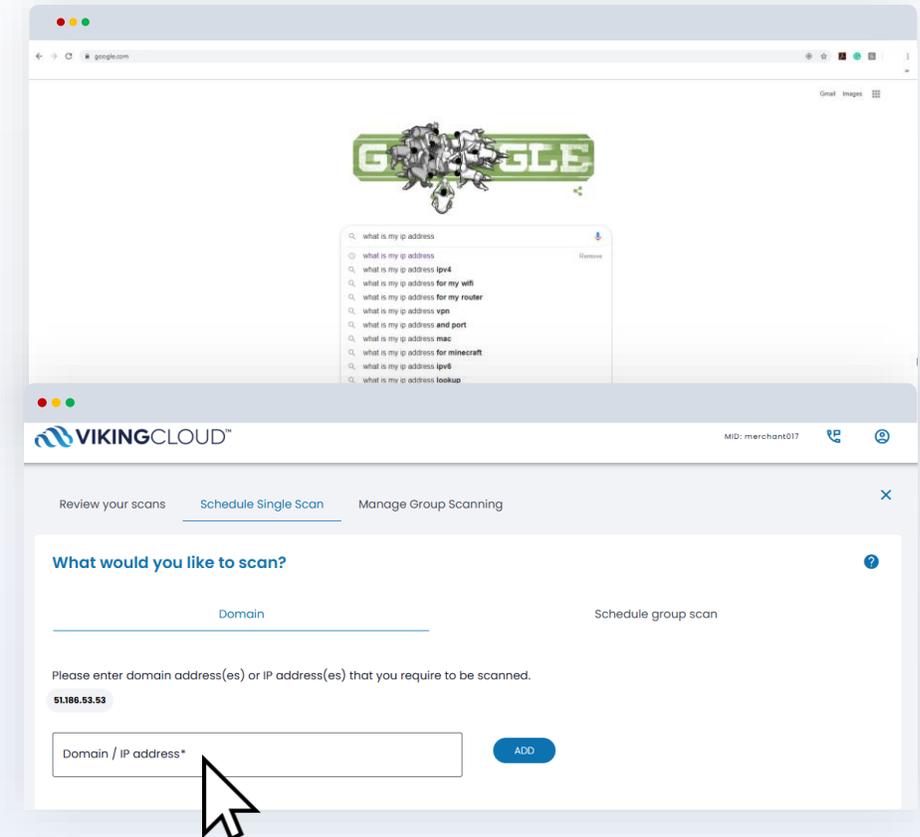
- Connect a laptop, desktop or mobile device to the same network that your card payment machine is connected to. This may mean disconnecting your card machine and plugging in either your laptop or other device.
- Open your preferred search engine or browser and search “What is my IP address”

Quick note: It is the IPv4 address that is needed, not the IPv6. The IPv4 address will be a series of numbers separated by dots (e.g., 123.123.123.123. The IPv6 is a much longer and includes numbers and letters).

- Copy the IP address provided, paste into the space on the portal provided and select ‘Add’.

There are two main public IP address types:

- **Dynamic IP:** This type automatically changes from time to time. Before each scan, you will need to find your current, public IP address for the connection that your payment terminal is using – following the steps above.
- **Static IP:** This type remains constant. If your business has a static public IP, you can save your IP address on the portal for future scans, you don’t need to search for it each time.



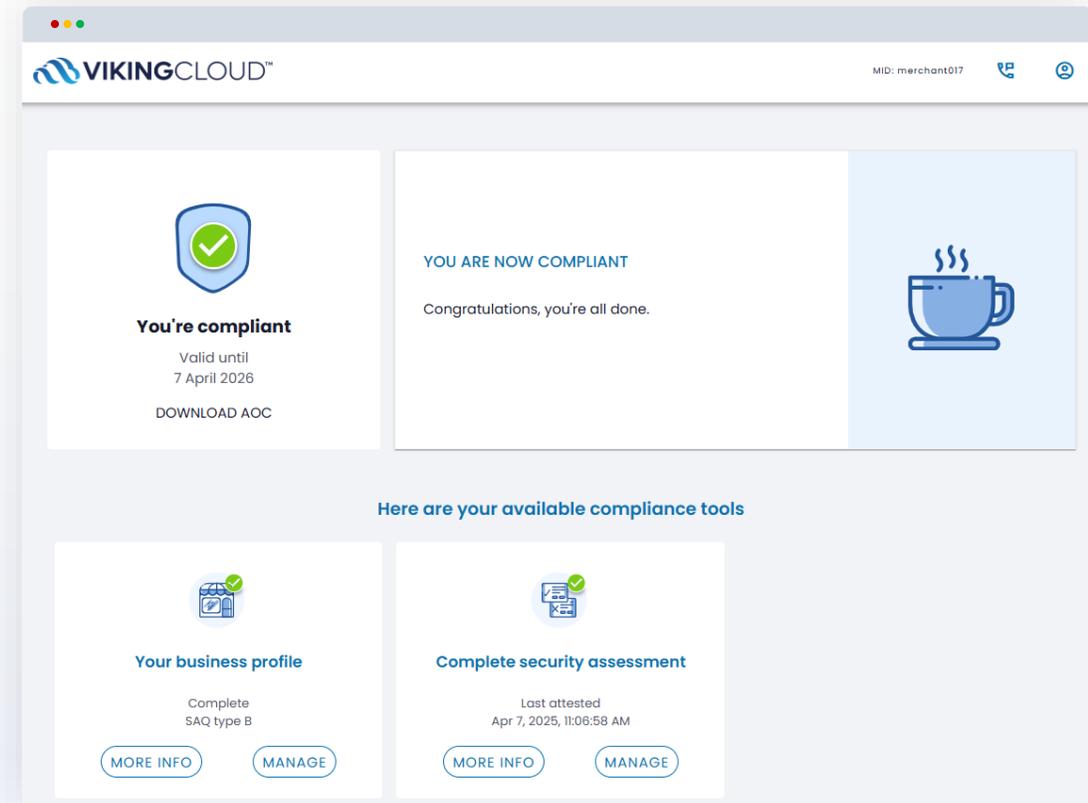
Validation complete – downloading your documents

Your revalidation date is displayed in the top left corner.

You can download your Attestation of Compliance by clicking on the **“Download AOC”** link.

This is your official PCI DSS compliance attestation document. Confirming your ongoing commitment to maintaining your compliance with the PCI DSS.

Throughout the year, we will email you as and when tasks are due, and when your next revalidation date is approaching.



A man with glasses and a woman are smiling and looking at a tablet together. They are in a bright, modern office or library setting with bookshelves in the background. The man is wearing a pink shirt and the woman is wearing a striped shirt. The background is slightly blurred, showing other people working at desks.

Merchant User Guide

Thank You

V1.0 Latest Update December 2024