Merchant
User Guide

Updated April 2025

Merchant User Guide

What is PCI DSS

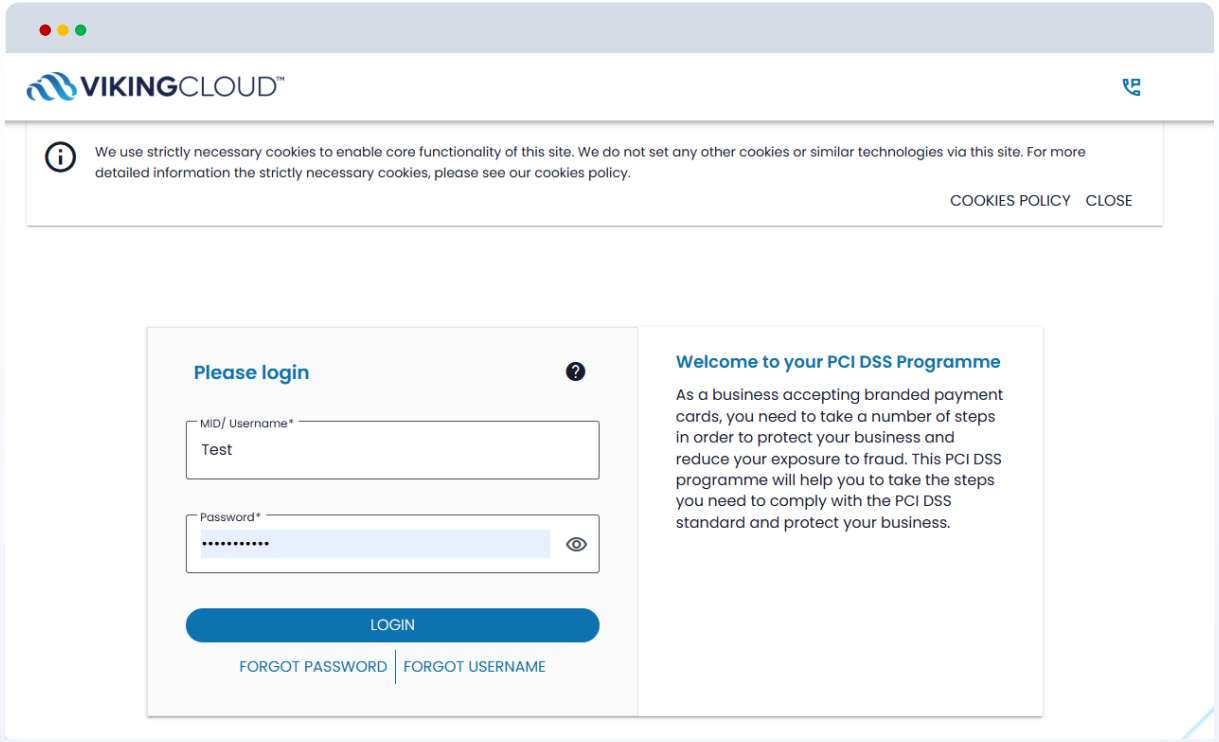
The PCI DSS is a set of security standards designed to protect your customers' credit card information. It is a checklist of things you need to do to keep your business safe from cyberattacks.

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.



GO TO CONTENTS

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

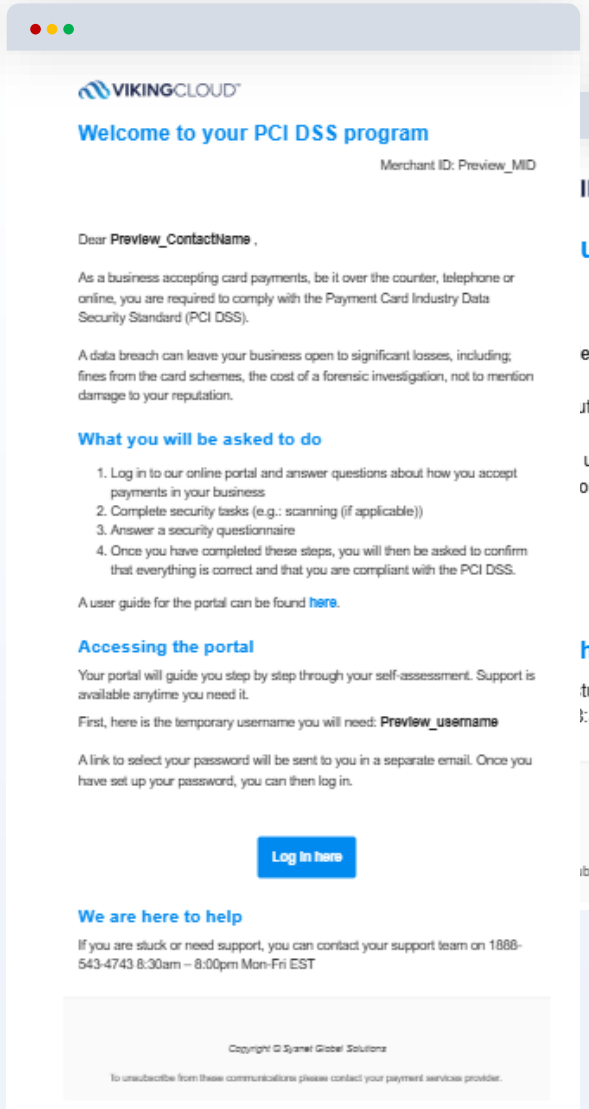
Getting started
- How to access the online portal

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.


VIKINGCLOUD

Welcome to your PCI DSS program

Merchant ID: Preview_MID

Dear **Preview_ContactName** ,

As a business accepting card payments, be it over the counter, telephone or online, you are required to comply with the Payment Card Industry Data Security Standard (PCI DSS).

A data breach can leave your business open to significant losses, including; fines from the card schemes, the cost of a forensic investigation, not to mention damage to your reputation.

What you will be asked to do

1. Log in to our online portal and answer questions about how you accept payments in your business
2. Complete security tasks (e.g.: scanning (if applicable))
3. Answer a security questionnaire
4. Once you have completed these steps, you will then be asked to confirm that everything is correct and that you are compliant with the PCI DSS.

A user guide for the portal can be found here.

Accessing the portal

Your portal will guide you step by step through your self-assessment. Support is available anytime you need it.

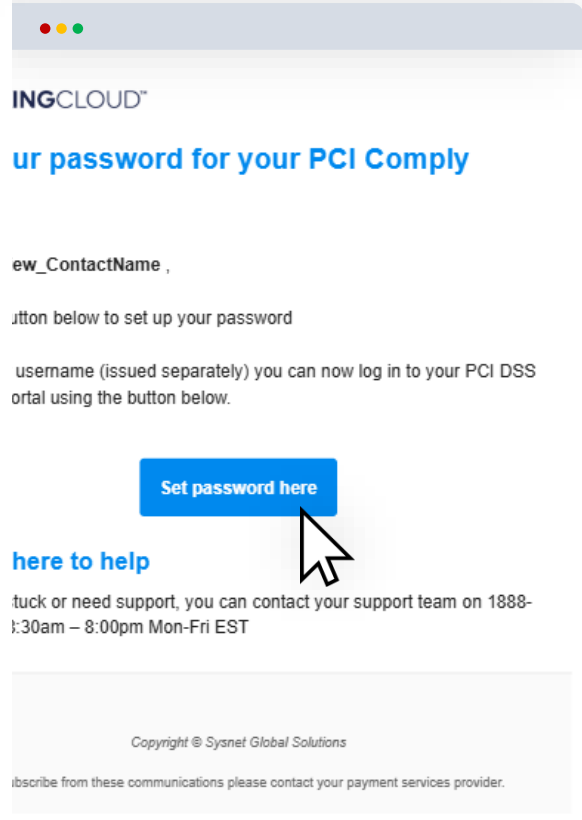
First, here is the temporary username you will need: **Preview_username**

A link to select your password will be sent to you in a separate email. Once you have set up your password, you can then log in.

Log in here

We are here to help

If you are stuck or need support, you can contact your support team on 1888-543-4743 8:30am – 8:00pm Mon-Fri EST


INGCLOUD

ur password for your PCI Comply

ew_ContactName ,

utton below to set up your password

username (issued separately) you can now log in to your PCI DSS ortal using the button below.

Set password here

here to help

tuck or need support, you can contact your support team on 1888- :30am – 8:00pm Mon-Fri EST

Copyright © Sysnet Global Solutions

ubscribe from these communications please contact your payment services provider.

GO TO CONTENTS >

Your starting dashboard

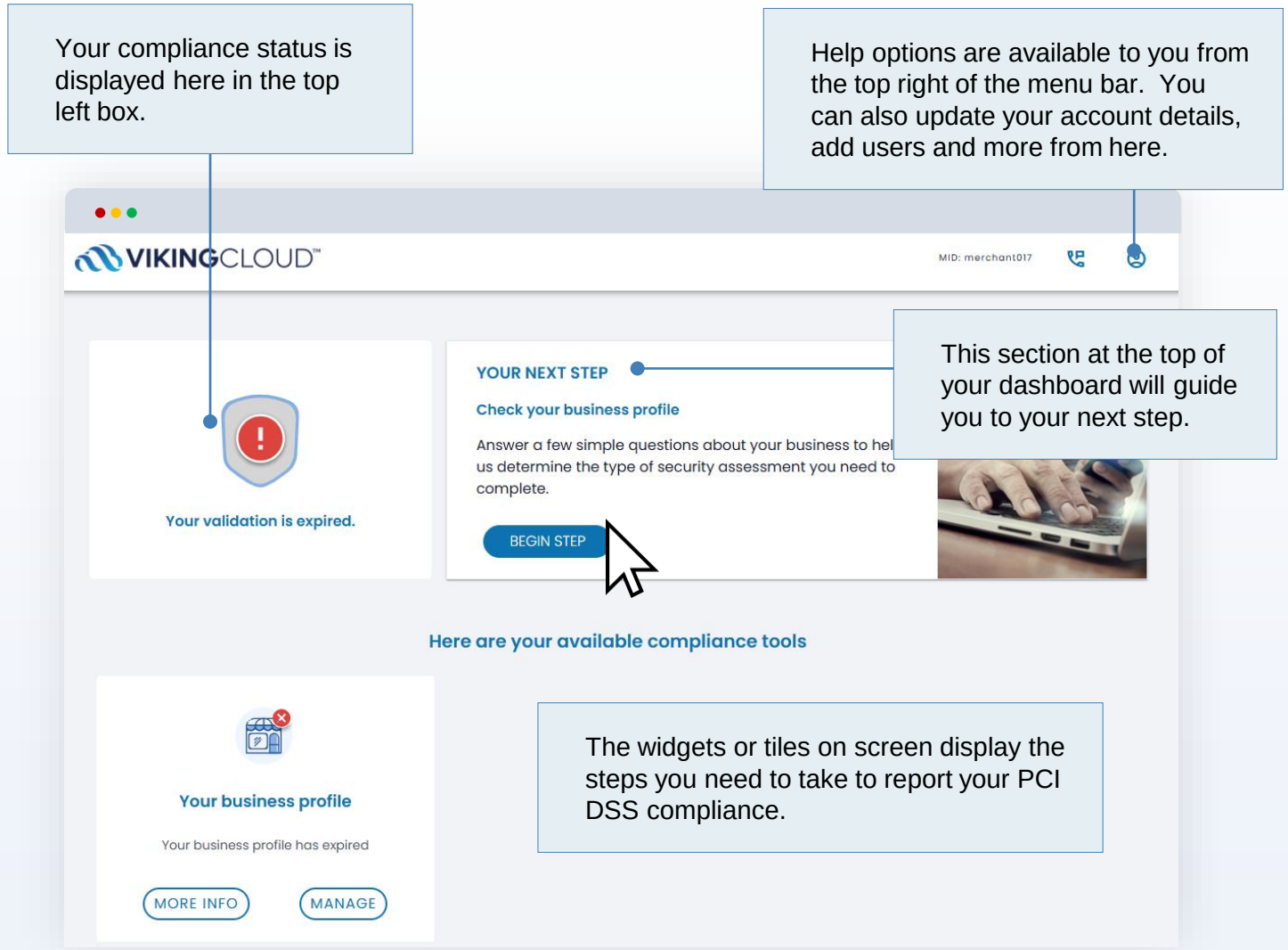
Once logged in, you will land on your dashboard.

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.



GO TO CONTENTS

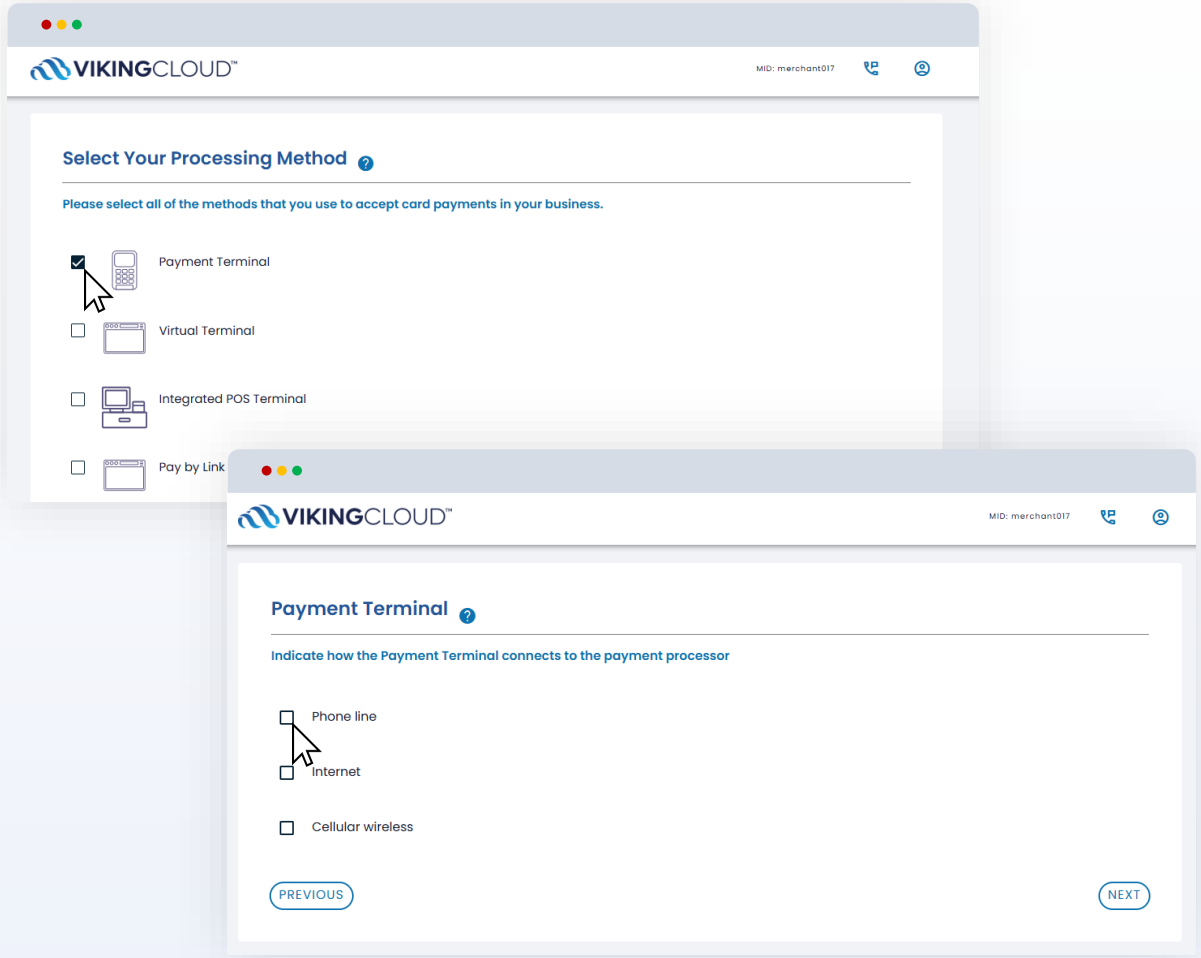
Your business profile – what you need to know:

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.

GO TO CONTENTS >

Your business profile
Information Security Policy

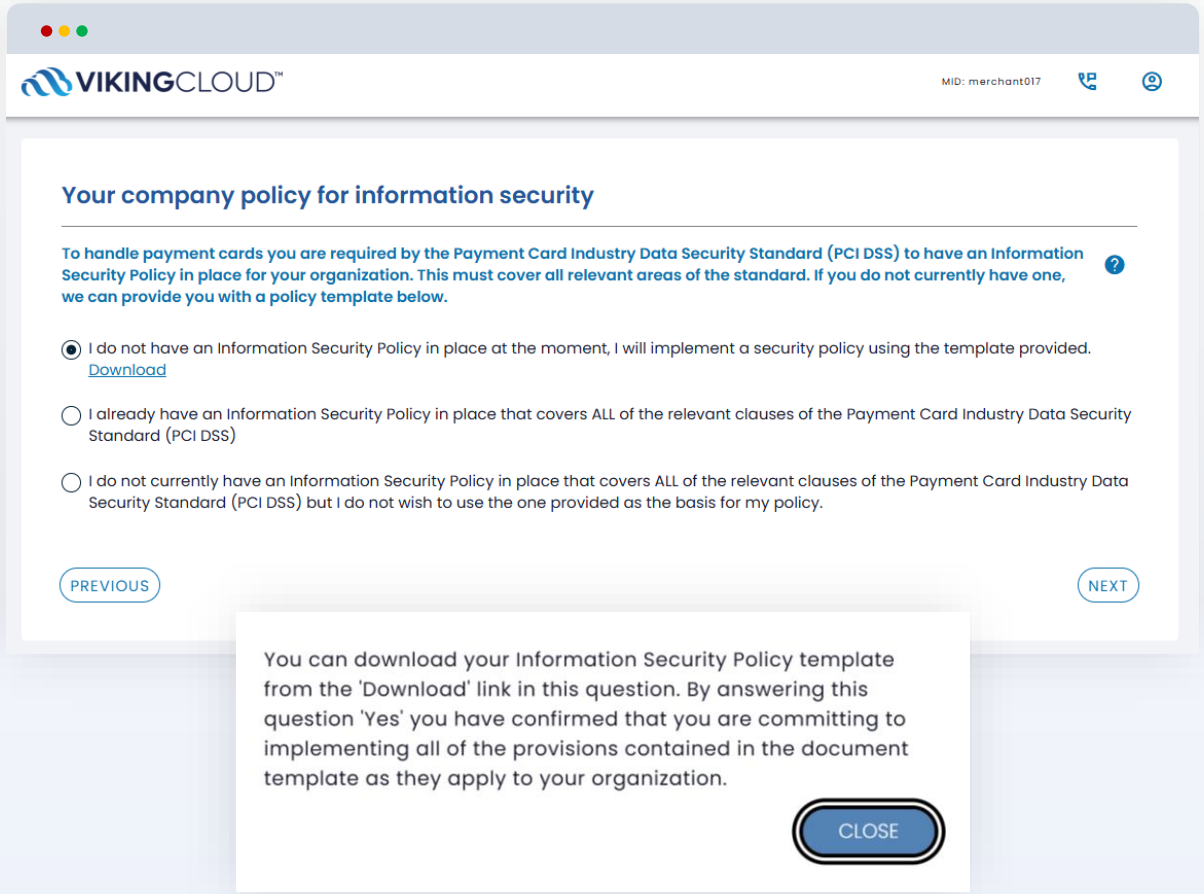
As part of maintaining your PCI DSS compliance – it is mandatory that you have an Information Security Policy.

- 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.



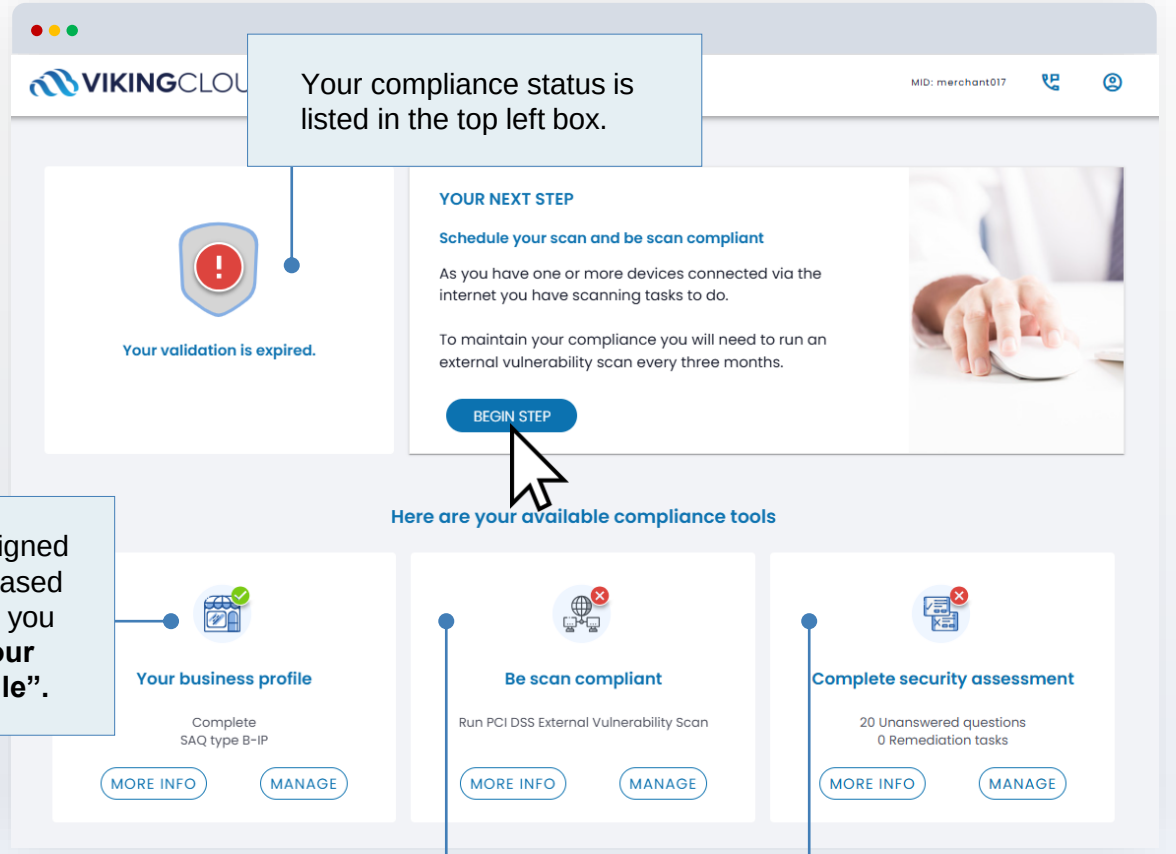
GO TO CONTENTS >

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.



Your compliance status is listed in the top left box.

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’.**

GO TO CONTENTS >

Complete security assessment
– (Self-Assessment Questionnaire section)

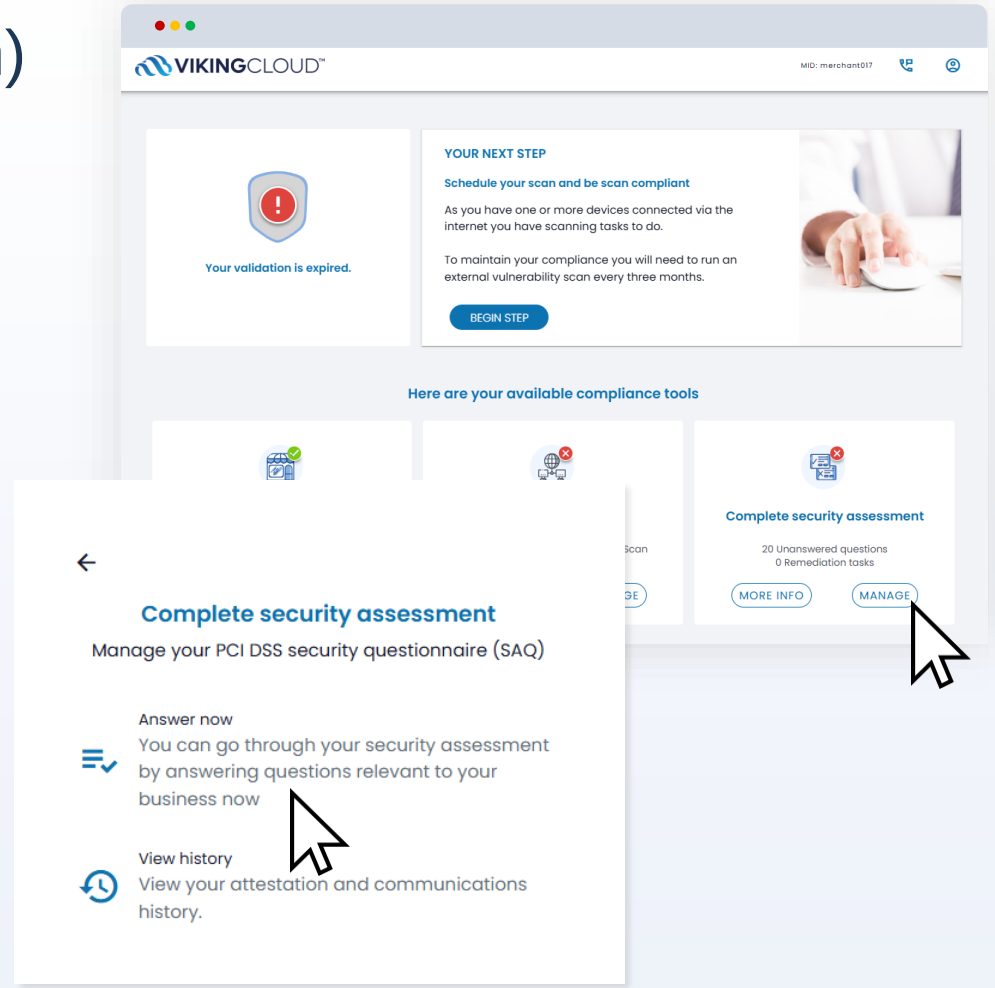
Your remaining PCI DSS Payment Card Industry Data Security Standard (PCI DSS) requirements and attestation steps are available for completion via the **“Complete security assessment”** widget.

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.

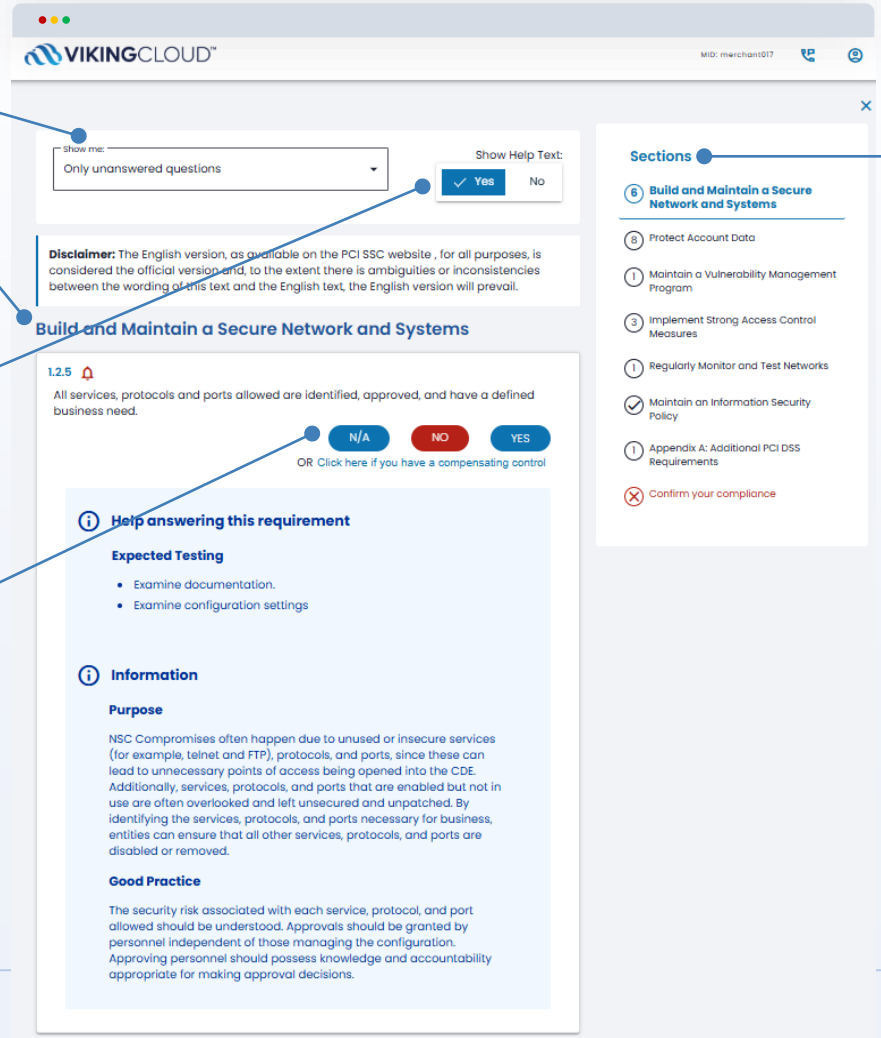


Complete security assessment
– (Self-Assessment Questionnaire section - (SAQ))

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.



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.

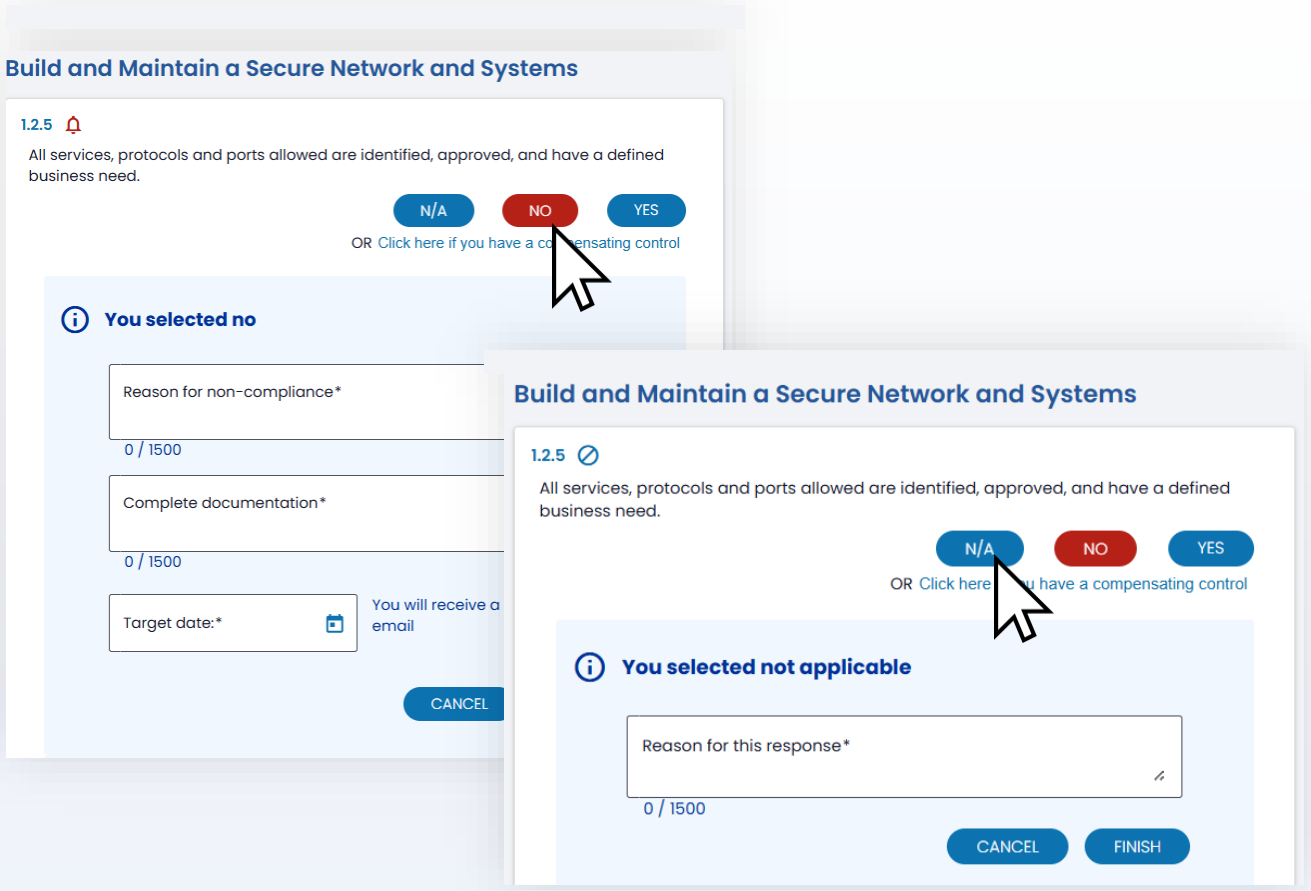
Complete security assessment – (Self-Assessment Questionnaire section - (SAQ)

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.



Complete security assessment – Attestation

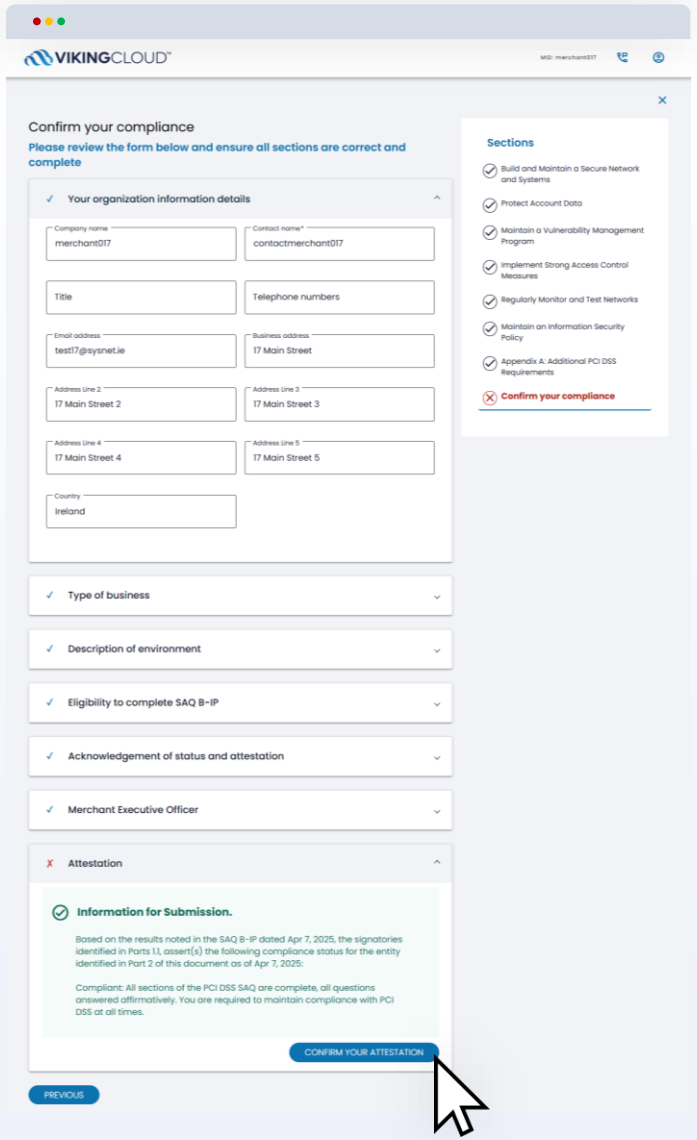
Once you have answered all sections and requirements, the next step is for you to attest to your compliance.

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.

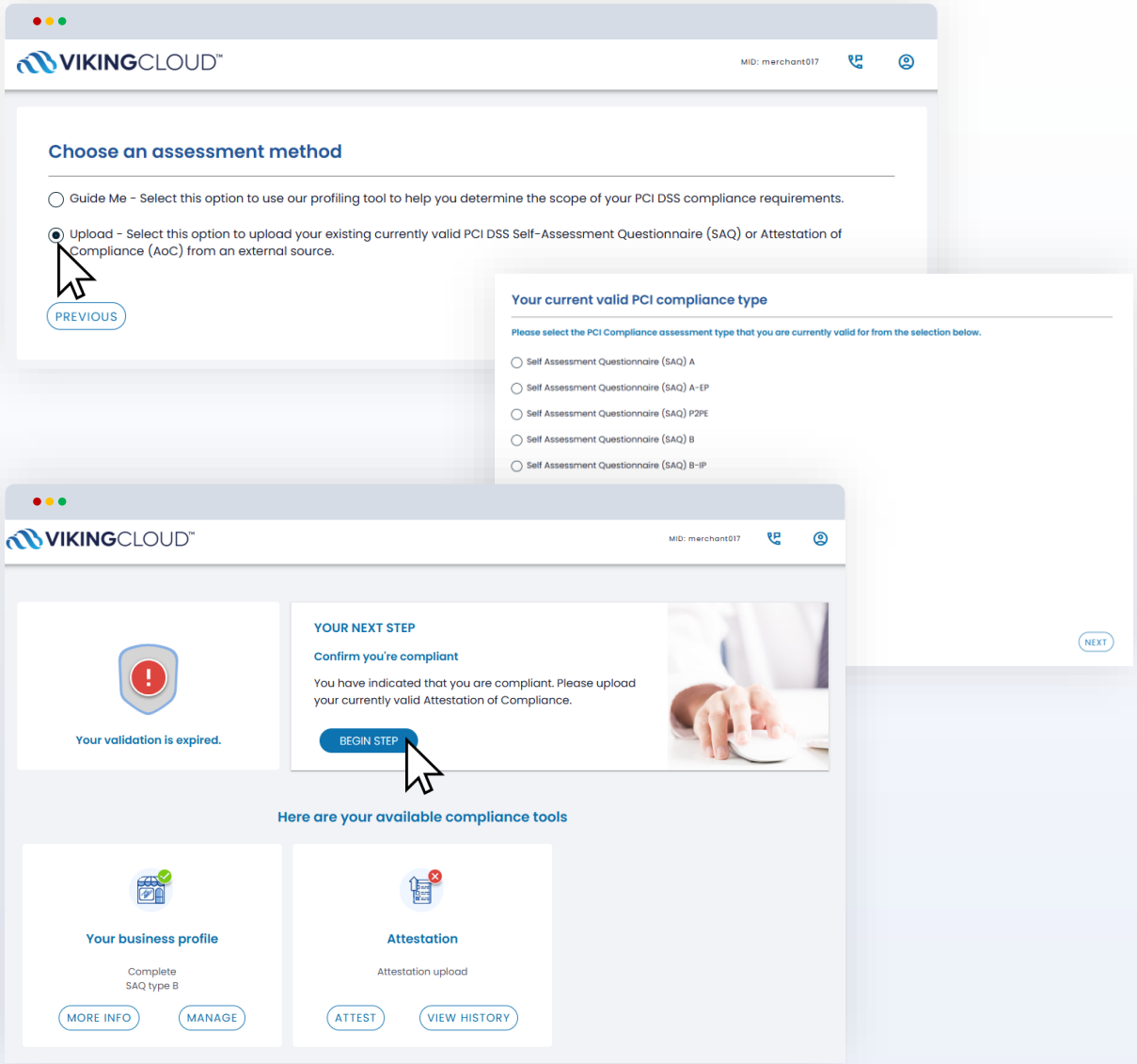


GO TO CONTENTS

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).

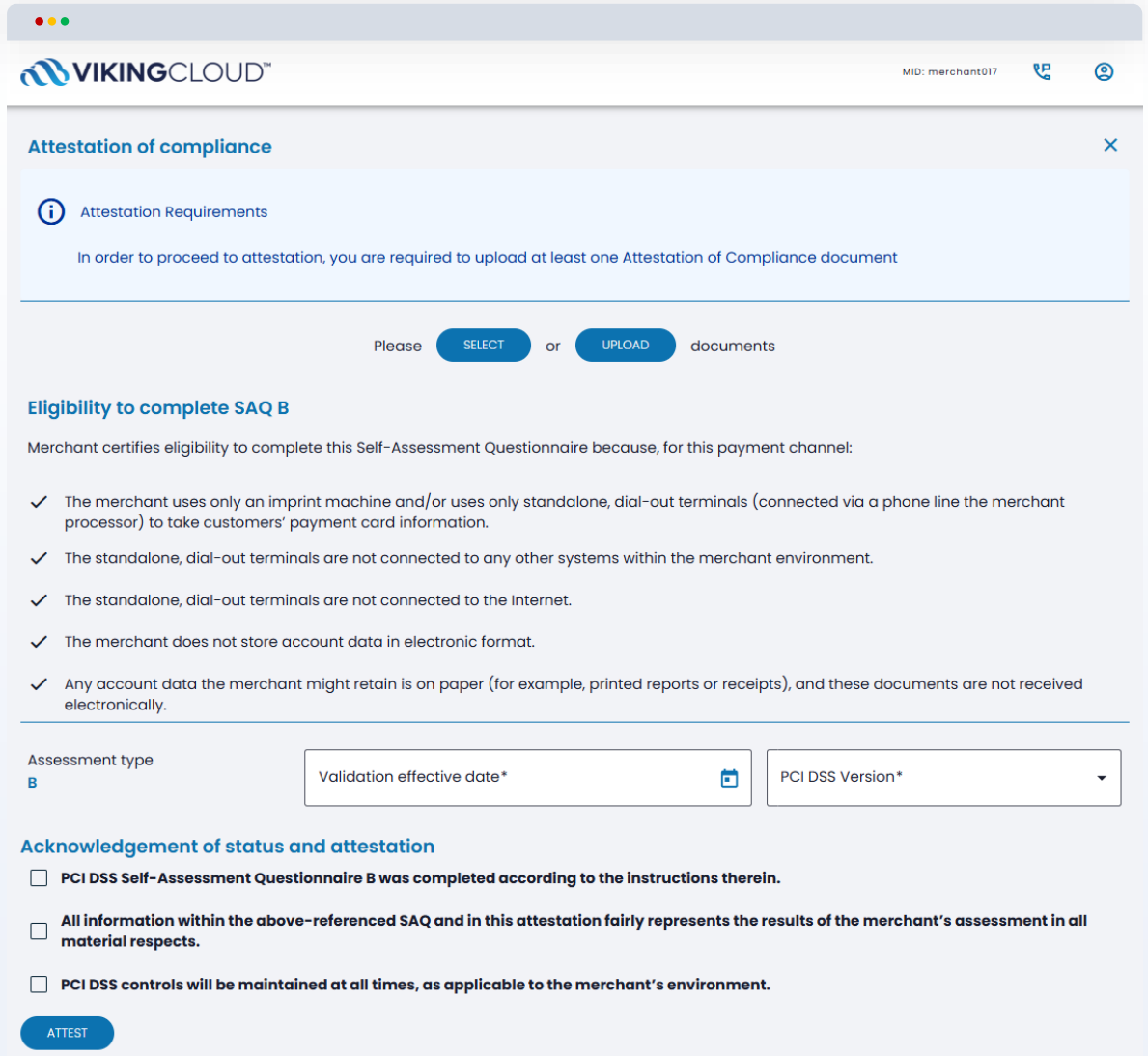


GO TO CONTENTS

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.



GO TO CONTENTS >

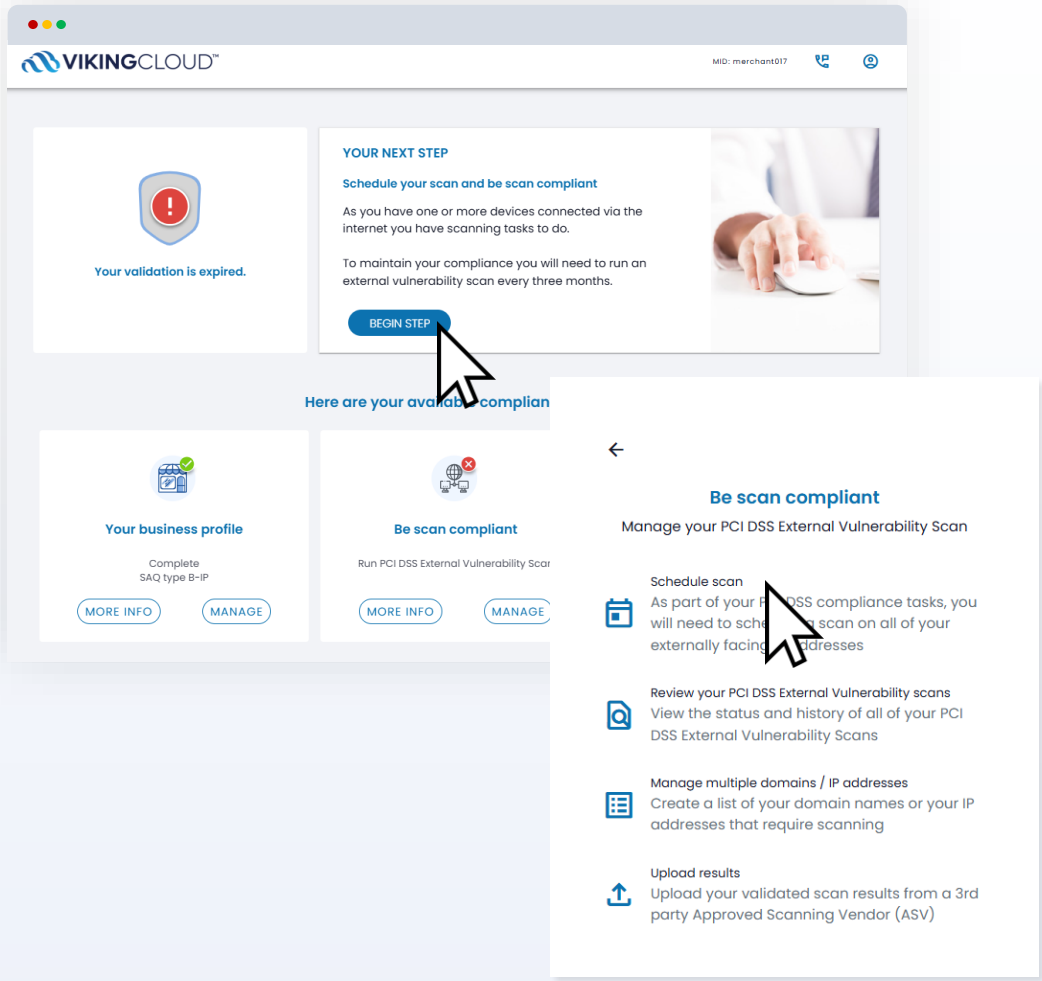
Be scan compliant – External Vulnerability Scanning

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

Or you **“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.



GO TO CONTENTS

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.

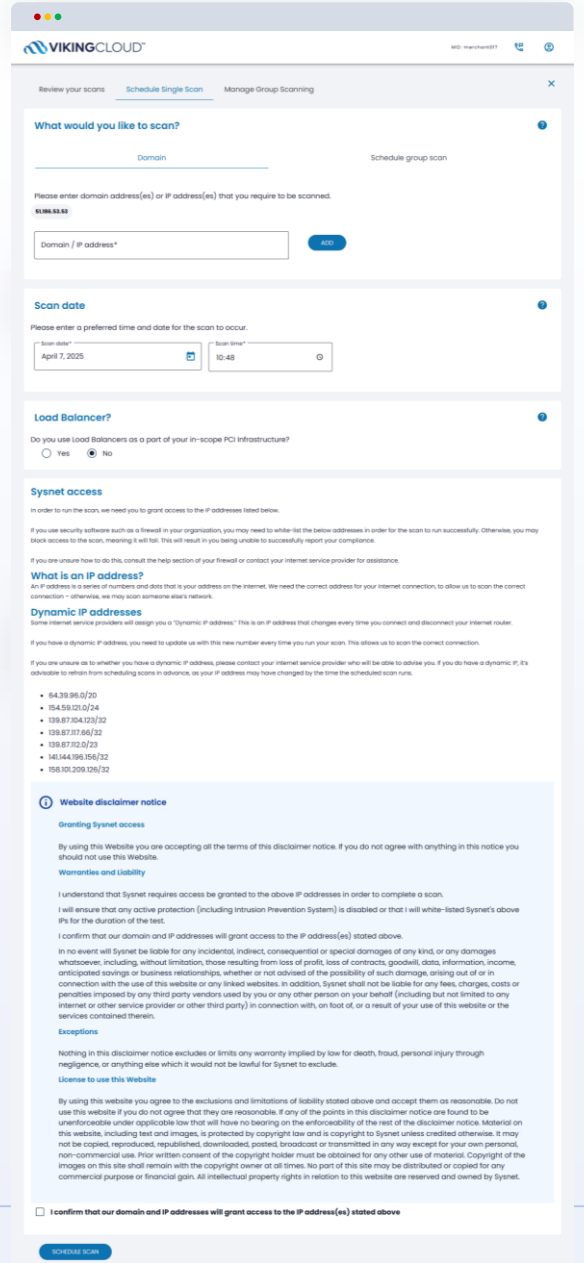
"Scan date": We recommend setting this to the current time and date for the scan to enter the queue.

"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 scam, 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.



GO TO CONTENTS

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:

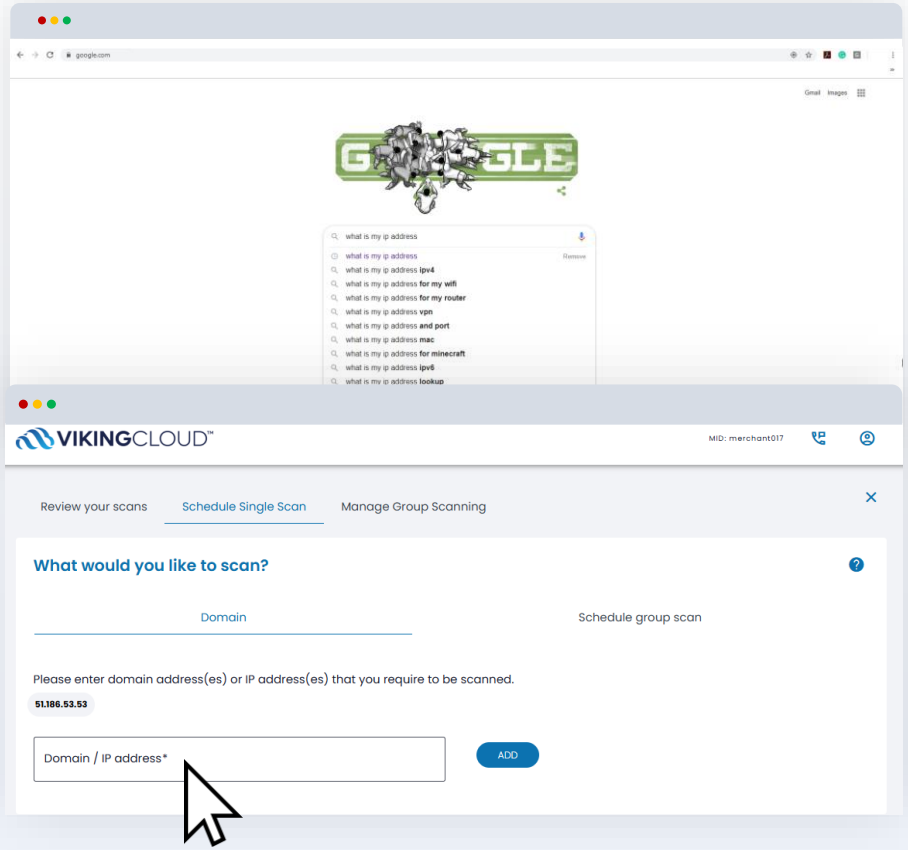
- Connect a laptop, desktop or mobile device to the same network that your card payment machine is connected to. This may mean disconnecting your card machine and plugging in either your laptop or other device.
- Open your preferred search engine or browser and search “What is my IP address”

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.



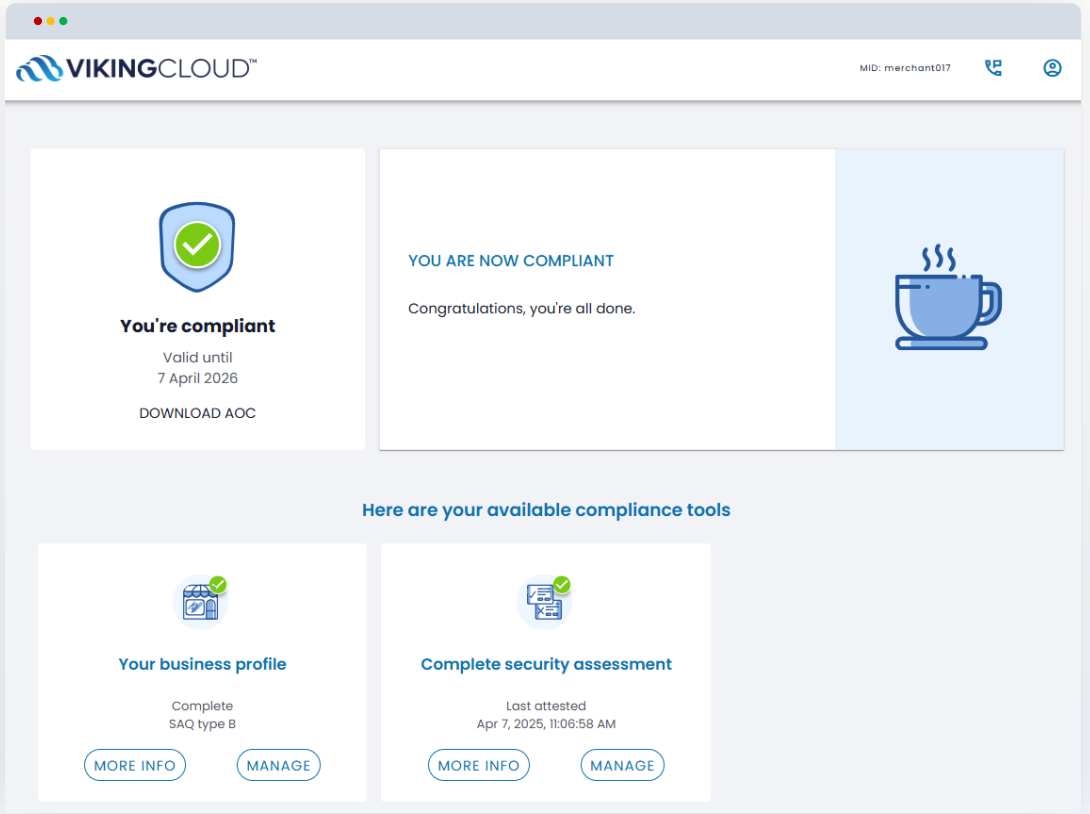
Validation complete – **downloading your documents**

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.



Merchant User Guide

Thank You

V1.0 Latest Update December 2024