

The background of the slide features a network of interconnected nodes and lines, with a color gradient from dark blue on the left to light green on the right. The nodes are represented by circles of varying sizes and colors, including teal, light green, and dark green. The lines are thin and light green, creating a complex web-like pattern across the entire slide.

SecureTrust™

PCI Portal

User Guide for Merchants

Table of Contents

- 3 What's included?
- 4 The process
- 5 Login
- 6 Your profile
- 12 Your dashboard
- 16 Scanning
- 20 Security Assessment Questionnaire (SAQ)
- 27 You're done for now
- 28 Upload an existing certificate



What's Included?

- **Report your PCI DSS compliance**
 - Streamlined and simplified journey
 - Download your information security policy template
- **Maintain your compliance throughout the year**
 - Login to complete regular scanning and maintenance tasks
- **Receive email alerts and reminders so you always stay up to date**
- **Rich online, chat and phone support available if you get stuck**

The Process

1

Login

Login to the portal and change your password

2

Profile

Complete your business profile by answering questions on how you accept payments

3

Scanning

Complete scanning on your network if applicable to your business profile type

4

Security Assessment

Complete your Security Assessment Questionnaire (SAQ) – an online assessment of your security practices

5

Maintenance

You may need to maintain your compliance. We'll remind you by email if this is the case.

Login

- Upon first logging in to the portal, use the username and password provided in your emails and click 'Login'.
- You will then be prompted to update your password. Your password will need to meet the minimum-security criteria outlined on the screen.
- Once you have completed this, you will be brought to an information page that gives you an overview of what you need to do and an information video.
- **Note: If you did not receive a welcome email, you can select the register button once you have confirmed your MID is already enrolled into the PCI program**

SecureTrust
is now vikingCLOUD™

! Your portal experience has been updated to reflect the new requirements of the PCI DSS version 4.0. You can find out more about PCI DSS version [here](#). DISMISS

Please login ?

MID/ Username*
test

Password*
••••••••

LOGIN

FORGOT PASSWORD | FORGOT USERNAME

First time logging in?

REGISTER

Welcome to the SecureTrust Portal

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

PASSWORD UPGRADE
Please note that you will need to reset your password if you have not signed into the portal since March 24th, 2022. Please click 'FORGOT PASSWORD' and follow the instructions provided.



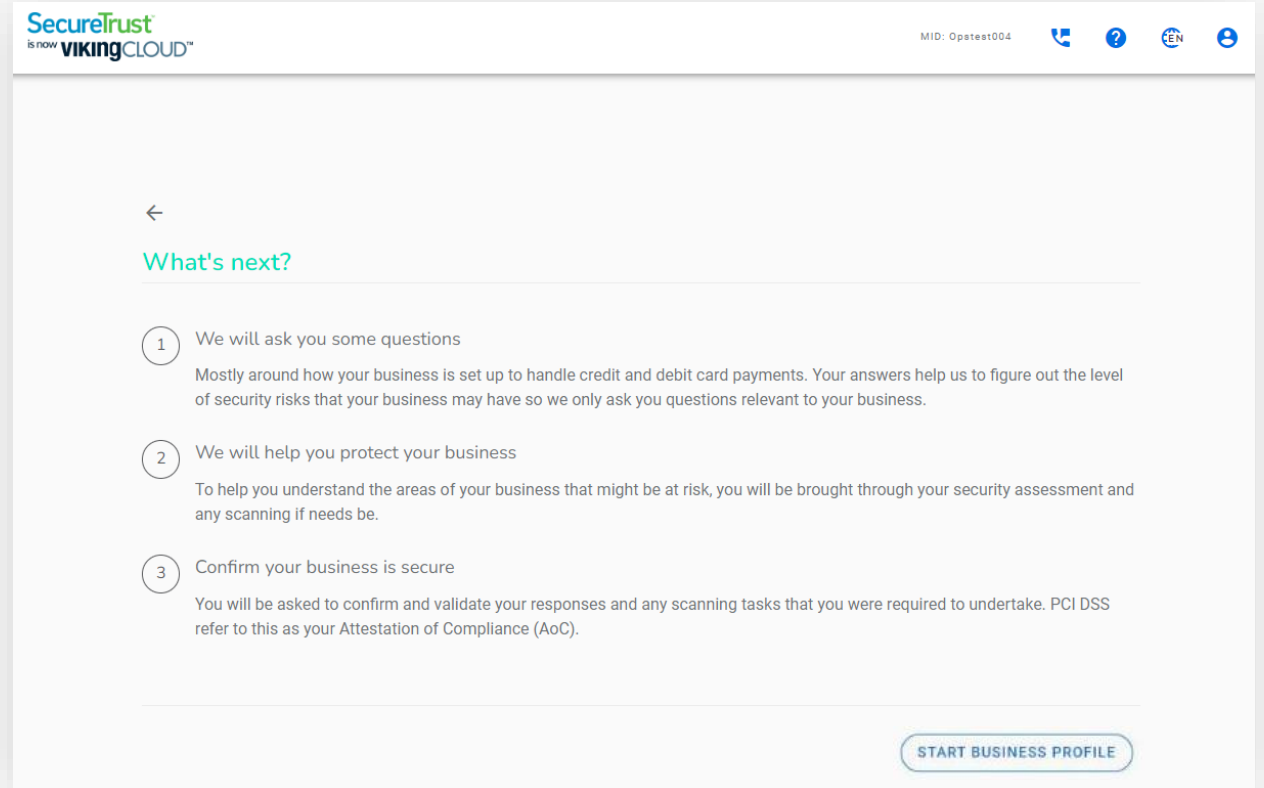
Your Profile

How you accept payments



Start Business Profile

- Once logged in, you will be brought to an information page that gives you an overview of what you need to do and a short information video.
- Click 'Start Business Profile' to begin.



PCI DSS v4.0

- You will be presented with a notification regarding PCI DSS v4.0. Here you will need to select the box to confirm you understand what the introduction of this new standard means for your compliance.

SecureTrust™
is now **VIKING**CLOUD™

MID: Opstest004



PLEASE READ: PCI DSS 4.0 update

We have updated our profile process to comply with the requirements of version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS).

If you have Payment terminals in use completed this process previously, please re-confirm your answers. You may be required to answer some additional questions in order to correctly determine your compliance requirements under the latest version of the standard.

Please refer to the PCI Security Standards Council [PCI DSS v4.0 Resource Hub](#) for more information.

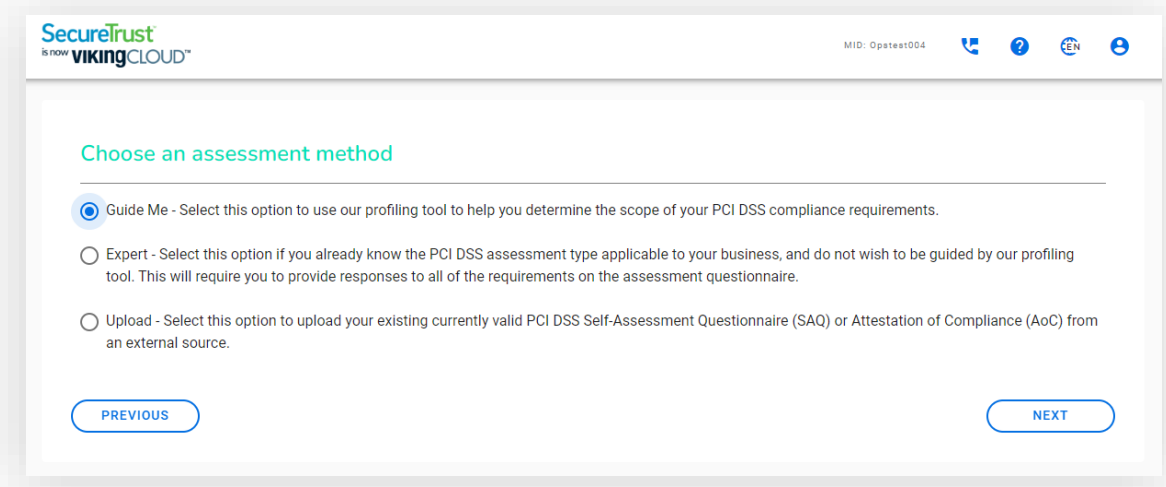
We have also made some additional resources available [here](#).

☐ I understand

NEXT

First time using the portal?

- The first screen you will encounter is a question as to whether you have completed this process before.
- In some cases, you may have already completed your PCI compliance with an assessment company. If this is the case, select "Upload" and proceed to page 28 of this guide for instructions on uploading your existing documentation.
- You also have the option to select 'Expert' allowing you to choose from a selection of PCI SAQ forms.
- **If you do not already have a valid certificate and need to complete your compliance online, select the first option on this screen and continue to page 9 of this guide.**



The screenshot shows the 'Choose an assessment method' screen in the SecureTrust portal. The header includes the SecureTrust logo, 'is now vikingCLOUD™', and a user ID 'MID: 0patest004'. There are four icons in the top right: a speech bubble, a question mark, a globe, and a user profile. The main content area has the title 'Choose an assessment method' and three radio button options:

- ☒ Guide Me - Select this option to use our profiling tool to help you determine the scope of your PCI DSS compliance requirements.
- ☐ Expert - Select this option if you already know the PCI DSS assessment type applicable to your business, and do not wish to be guided by our profiling tool. This will require you to provide responses to all of the requirements on the assessment questionnaire.
- ☐ Upload - Select this option to upload your existing currently valid PCI DSS Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) from an external source.

At the bottom, there are two buttons: 'PREVIOUS' on the left and 'NEXT' on the right.

Your Profile – How do you accept payments?

- You will be guided through some questions asking how you accept payments in your business.
- You will be asked questions about the technology you use as well as methods by which you may transfer or store data.
- Select the options that apply to your company and click through via the 'Next' buttons. You can select more than one option in many cases.
- If you are unsure about any of the options or need further clarification, more information is available by clicking the help icon found in the top right of the screen.

The screenshot shows a web interface for a questionnaire titled "How do you accept payment cards?". The header includes the "SecureTrust is now vikingCLOUD" logo and a user ID "MID: Opatest004". In the top right corner, there are icons for a telephone, a question mark (help), a globe (language), and a user profile. The main content area contains the question "How do you accept payment cards?" followed by instructions: "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, ApplePay and GooglePay are not applicable)". There are three options, each with an unchecked checkbox and a help icon: 1. "Face to face (the customer is present and the payment card is inserted, tapped or swiped to complete the transaction. This includes unattended kiosks.)" 2. "Online payments (incl. e-Commerce website/shop, consumer mobile app, etc.)" 3. "Mail and/or telephone order card payments". At the bottom of the form are two buttons: "PREVIOUS" on the left and "NEXT" on the right.

Your Profile – Payment Summary

- You will be asked to provide a summary of your payment acceptance processes.
- **You will be asked to:**
 - List your business premises and provide a summary of the locations where you accept payments
 - Explain how your business handles cardholder data
 - Provide a high-level description of how you accept payments
- Please provide as much information as possible. If you are stuck, help is available by clicking the help icons.

The screenshot shows a web form titled "A summary of how and where you handle card payments" under the SecureTrust logo. The form is part of an "Attestation of Compliance" and contains three text input fields, each with a "test" placeholder and a character count of "4/4000". The first field is for business premises, the second for cardholder data handling, and the third for a high-level business environment description. Each field has a help icon. Navigation buttons for "PREVIOUS" and "NEXT" are at the bottom.

SecureTrust
is now vikingcloud™

MID: Opates1004

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 centres, call centres etc.) ?

test

4/4000

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

test

4/4000

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 web servers, include a description as to how they connect both externally and any internal connections.

test

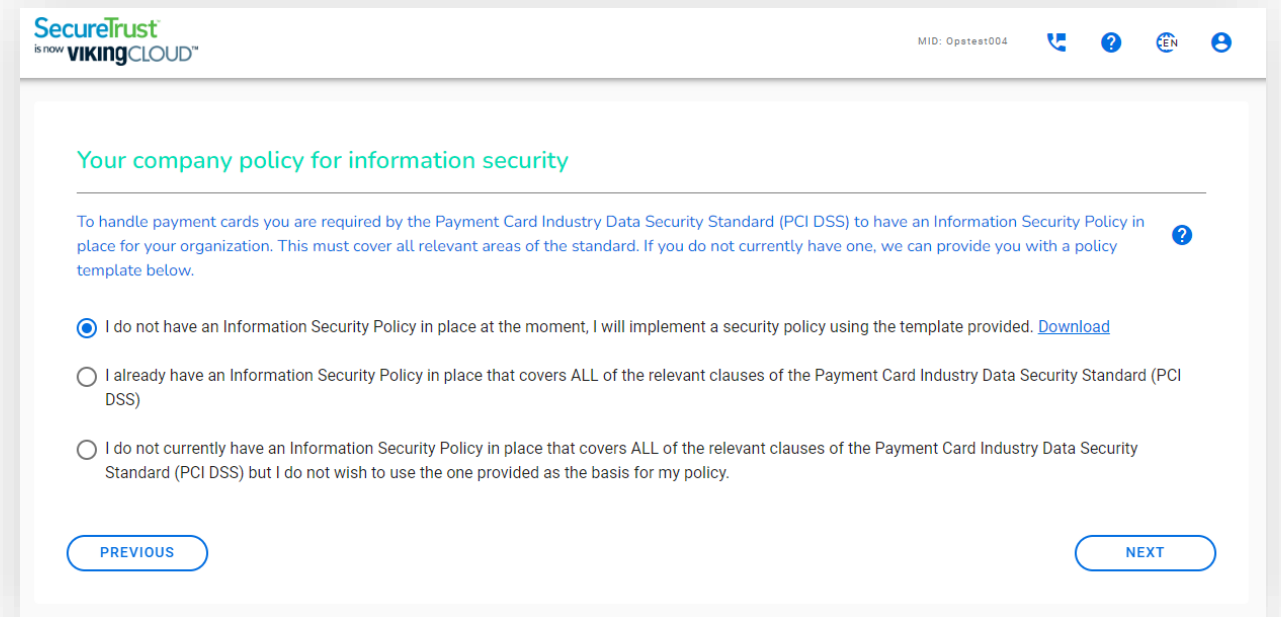
4/4000

PREVIOUS

NEXT

Your Profile – Information Security Policy

- It's mandatory to apply an Information Security Policy
 - This is a document that sets out the procedures you need to follow to handle information securely
- You will be asked if you have a policy in your business. If you don't, you can download a sample template by clicking 'I use the security policies included in my subscription'. Afterward you will answer additional questions on your information security policy.



The screenshot shows a web form titled "Your company policy for information security" under the SecureTrust logo (with the tagline "is now vikingCLOUD™"). The form includes a header with the user ID "MID: Opatest004" and navigation icons. The main text explains the requirement for an Information Security Policy (ISP) to handle payment cards according to the PCI DSS. It provides three radio button options: 1) "I do not have an Information Security Policy in place at the moment, I will implement a security policy using the template provided." with a "Download" link; 2) "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)"; and 3) "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." At the bottom, there are "PREVIOUS" and "NEXT" buttons.

SecureTrust
is now vikingCLOUD™

MID: Opatest004

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](#)



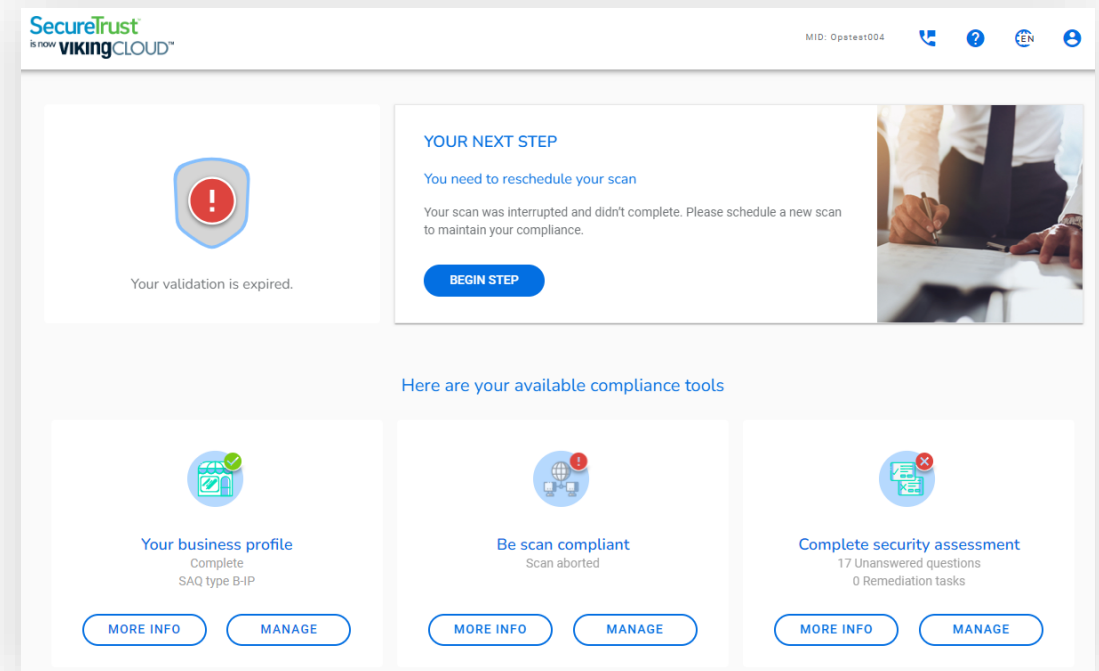
Your Dashboard

You have completed your profile journey



Your Dashboard

- Now that you have answered your profile questions, you will be presented with your dashboard.
 - From here you can complete your security assessment as well as any other tasks that are assigned to you following your questions (e.g., scanning).
 - Your security assessment will be based on the profile type assigned to you.
- You can read more information on how this works via the 'More Info' button on the 'Your business profile' widget.
- If the scanning widget appears, you must complete a scan by selecting 'Manage' from this widget.
- If you do not require a scan, or have completed one, you can begin your security assessment by clicking 'Manage' on the relevant widget.



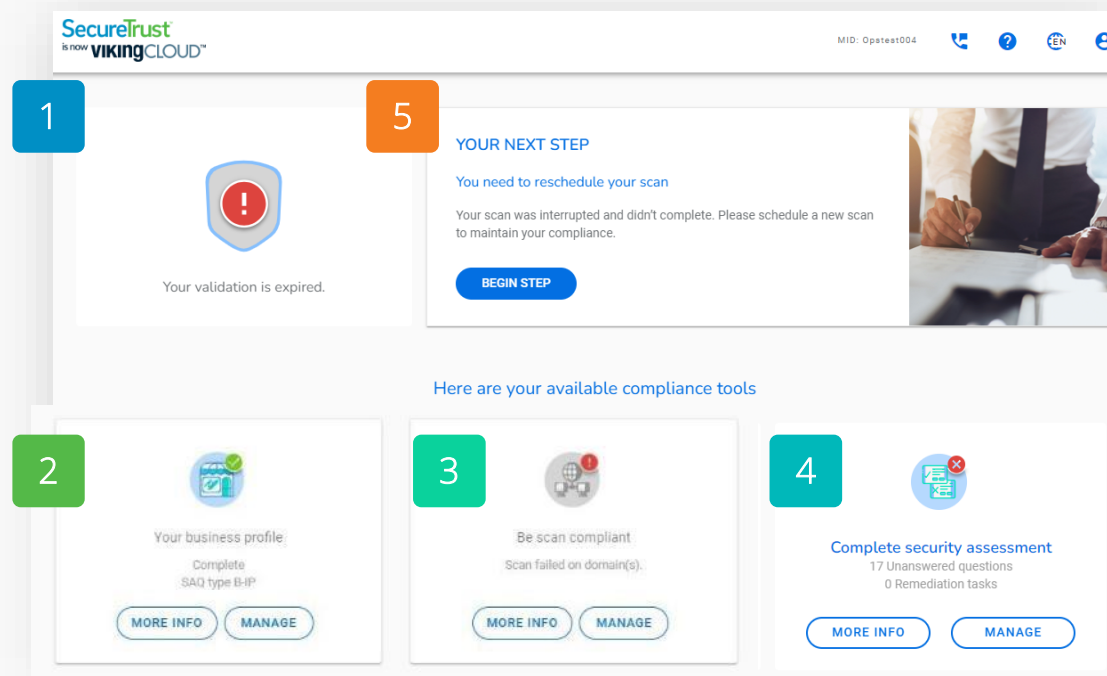
Your Dashboard

1

Your compliance status is listed at the top. You will not yet be compliant as you won't have completed your scanning (if applicable) or Security Assessment yet.

2

You will have been assigned a business profile type, based on the answers you provided in your questions. You can read more on what this means by clicking 'More Info'.



3

If applicable, you can conduct your scanning from here. Click 'Manage' on the scan widget to begin.

5

By clicking 'Your Next Step' you will be brought to your current stage of your compliance journey.

4

When you have completed your scanning (if applicable) you can proceed to your security assessment by clicking 'Manage'.

Next Steps

Scanning

If applicable to you, you will need to run a scan on your network. Proceed to page 16 for instructions.

Security Assessment

If don't have to do a scan, you can proceed to your security assessment on page 20.



Profile



Scanning – **Page 16**



Security Assessment – **Page 20**



Compliance



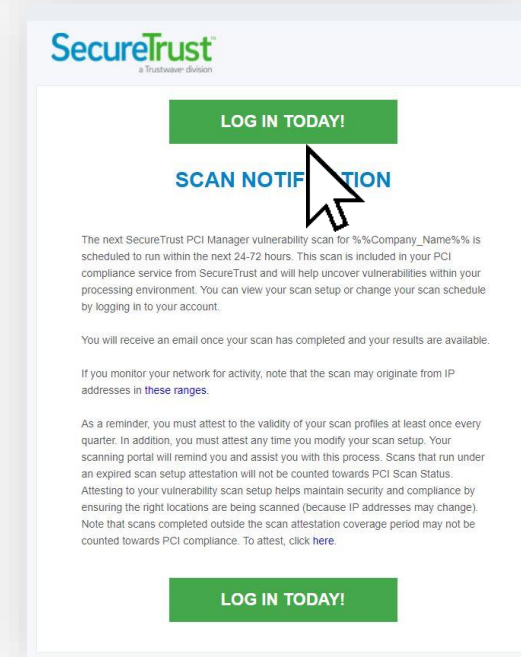
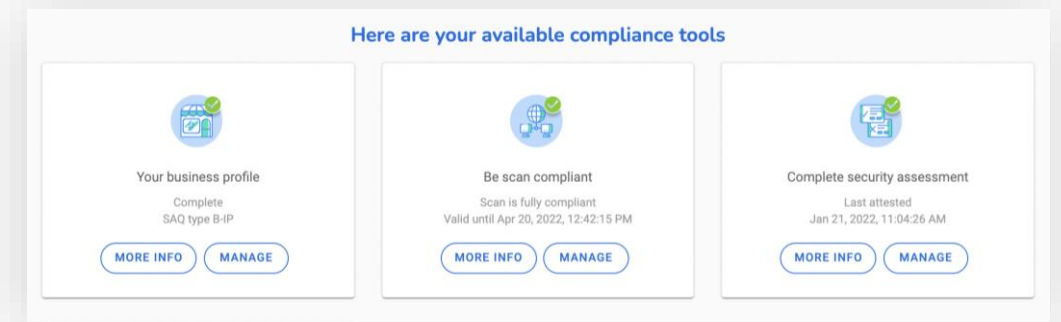
Scanning and SAQ

Carrying over your scanning and SAQ completion



Scanning and SAQ

- As part of the upgrade, your scan status, scanning targets, historical completed scans and SAQs have been transferred to the upgraded portal automatically.
- If you successfully completed your scan and/or SAQ prior to upgrade, you will see green checkmarks across your dashboard.
- When your scan is due you will be sent a scan notification email. Once received, you can quickly log in and run your scans.
- **Note:** Due to the upgrade, your scans will run on a quarterly basis as opposed to monthly.



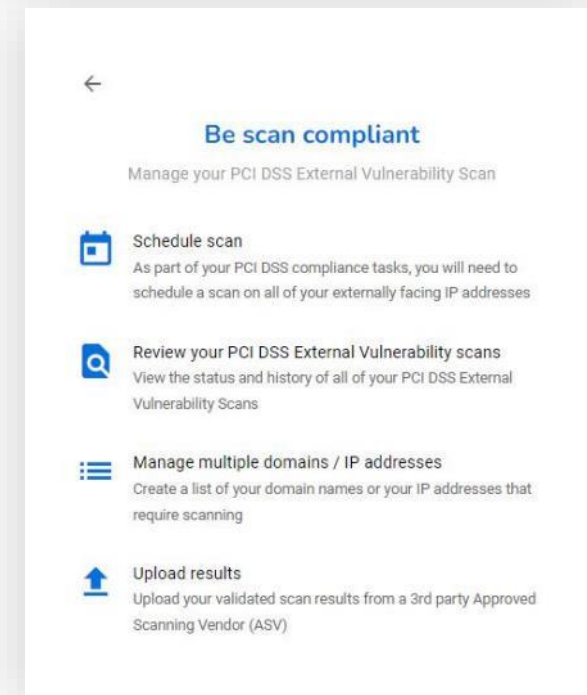
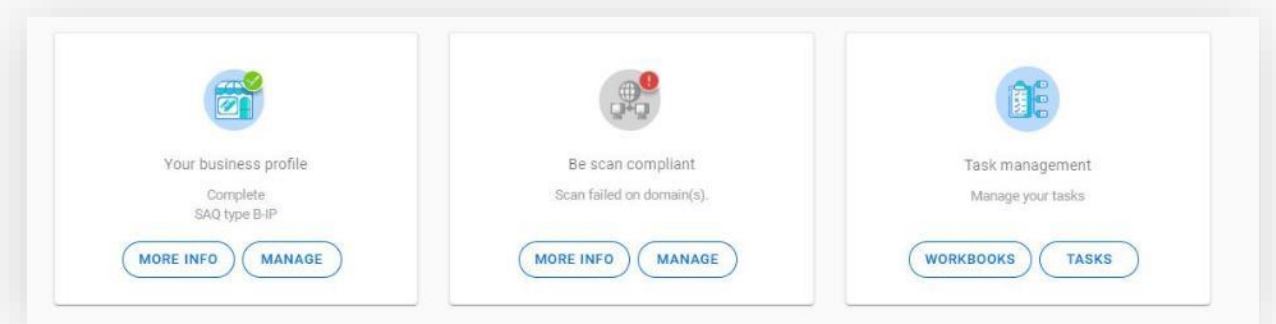


External Vulnerability Scanning



Scanning

- From your dashboard, select 'Manage' on the 'Be scan compliant' widget.
- On the next page, select 'Schedule scan'.



Scanning

- On the next screen you will need to input some details as follows:
 - The IP address.** This must be the same IP address as used by your card payment machine. Instructions on how to find this is available on the next page.
 - Scan date.** It will default to the current date and time. You can change this if necessary
 - Confirmation of whether you use a **load balancer**
- Once complete, select 'Schedule Scan'
 - The scan will then run and can take up to 48 hours. You will receive an email when the scan is complete.
 - You will be notified if remediation action is needed via your dashboard.
 - If your scan fails, you will need to complete the recommended remediation and then rerun the scan until a passing grade is achieved.

SecureTrust™ vikingCLOUD™

Review your scans | **Schedule Single Scan** | Manage Group Scanning

What would you like to scan?

Domain

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

87.196.219.176

Domain / IP address*

Scan date

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

February 23, 2024

09:11

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 to grant access to the IP addresses listed below.

If you use security software (e.g. firewalls) in your organization, you may need to whitelist 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.

64.39.96.0/20
139.87.112.0/23

Website disclaimer notice

Starting 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.

Warranty 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 whitelist Sysnet's above IP's 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.

Exemptions

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

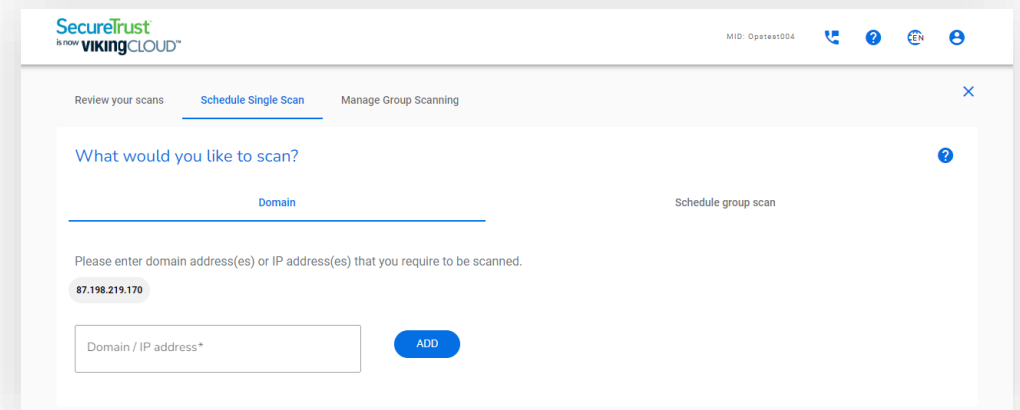
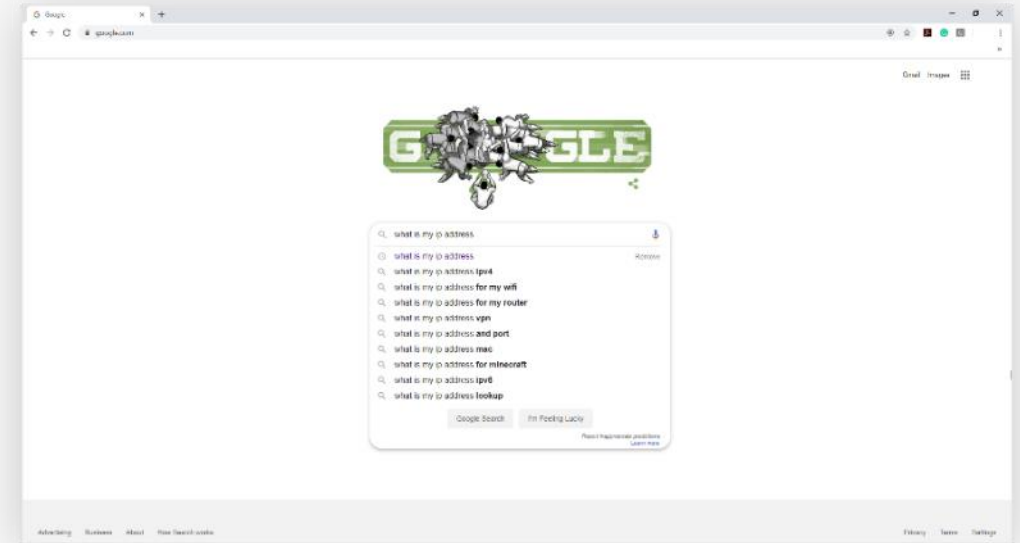
By using this website you agree to the exclusions and limitations of liability stated above and accept them as reasonable. Do not use this website if you do not agree that they are reasonable. If any of the points in this disclaimer notice are found to be unenforceable under applicable law that will 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

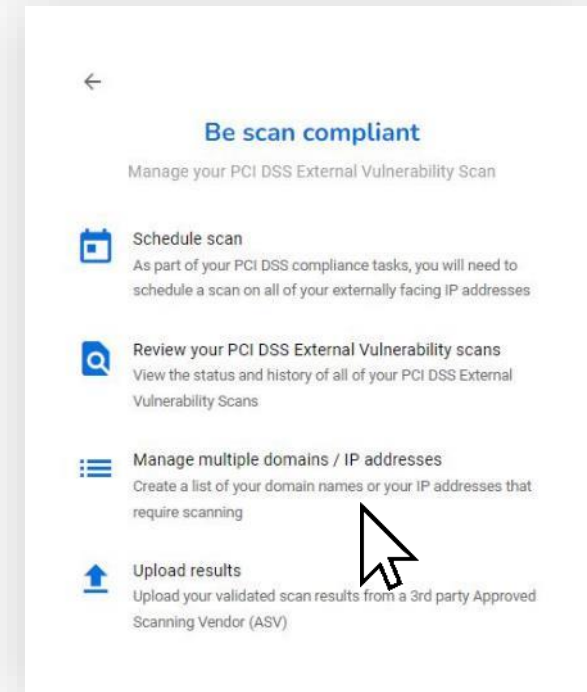
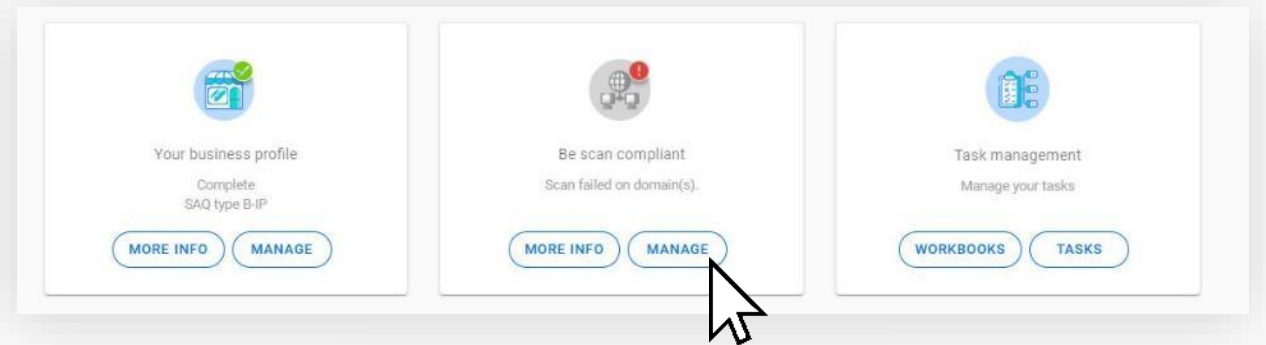
Finding your IP address

- To conduct a scan, you will need to provide us with your IP address. This 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 Wi-Fi network that your card payment machine is connected to
 - Open your preferred search engine or browser and search “What is my IP address”
 - You can find your address from the search results
 - Please note, it is the IPV4 address that is required, not the IPV6



Scheduling recurring scans

- To schedule recurring scans (monthly or quarterly) you will need to create a group to manage.
- Select manage and then manage multiple domains / IP addresses.



Scheduling recurring scans continued

- If you already have a group created you will see it listed here, if not, select '**Add a group**'.
- Select a group name and group type (Static IP addresses or dynamic) and click '**Submit**'.
- Once the group is added select your newly added group and chose '**Edit Group**'.

The first screenshot shows the 'Manage Group Scanning' page with a 'Group name' input field, a 'SUBMIT' button, and an 'ADD A GROUP' button. Below is a table with two rows of existing groups.

DATE CREATED ↓	GROUP NAME	GROUP TYPE	NUMBER OF DOMAINS / IP ADDRESSES IN GROUP	NEXT SCAN SCHEDULED FOR
Mar 4, 2024	test	Static IP addresses / domains only	0	
May 25, 2023	test group	Static IP addresses / domains only	0	

The second screenshot shows the 'Add a group' modal with 'Group name*' and 'Group type*' fields, and 'SUBMIT' and 'CANCEL' buttons.

The third screenshot shows the same table as the first, but with a 'Schedule' button and an 'Edit Group' button highlighted for the 'test group' row.

Scheduling recurring scans continued

- Select '**Add New Item**' and input the fields requested.
- Click 'Submit' when you're happy with the information provided.
- You will now need to click '**Schedule**' on the dropdown menu.

test
Static group

Schedule Edit Delete

Add New Item

Date created	Domain / IP Address	MID	Description
	Domain / IP Address		Description
No items to display			

Cancel Submit

Add a group

Date created	Group name	Group type	Number of domains / IP addresses in group	Next scan scheduled for
May 23, 2022	test	Static IP addresses / domains only	0	-
Apr 15, 2022	Static	Static IP addresses / domains only	2	-

Items: 2 / 2

Schedule Edit

Scheduling recurring scans continued

- Much like scheduling a once off scan you will need to select the scan date (your recurring scans will run from this date from your desired occurrence), whether or not a load balancer is present and finally give permission for the scan to run.
- You have the option to run a single, monthly or quarterly scan.

SecureTrust™
—wang—CLOUD™

With OpenSource

Review your scans Schedule Single Scan Manage Group Scanning

What would you like to scan?

Domain

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

Domain (IP address)*

Scan date

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

February 23, 2024 00:11

Load Balancer?

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

☐ Yes ☒ No

Sysnet access

In order to use the scan tool, you need to grant access to the IP address(es) listed below.

If you use security software, you may need to whitelist the below address in order for the scan to run successfully. Otherwise, you may block access to the scan, meaning it will fail. This is not a requirement for the scan to run successfully.

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 is advisable to refrain from scheduling scans in advance, as your IP address may have changed by the time the scheduled scan runs.

• 64.39.96.0/20
• 129.87.112.0/22

Website disclaimer notice

Starting 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.

Warranty and Liability

I understand that Sysnet requires access be granted to the above IP address(es) in order to complete a scan.

I will ensure that any active protection (including Intrusion Prevention Systems) is disabled or that I will whitelist Sysnet's above IP(s) for the duration of the test.

I confirm that our domain and IP address(es) 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 profits, 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.

Exclusions

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 indicated otherwise. It may not be copied, reproduced, republished, downloaded, printed, 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 address(es) will grant access to the IP address(es) stated above



Security Assessment Questionnaire

Your SAQ



Next Steps

Security Assessment Questionnaire (SAQ)

Your security assessment is an assessment of how you deal with information in your business. Its length and complexity depends on the results of your business profile.

Depending on your choice (guided or expert, explained on page 8) you will be provided with an SAQ that has prepopulated any questions that do not apply to you (guided), or a full SAQ containing all possible questions (expert).



Profile



Scanning



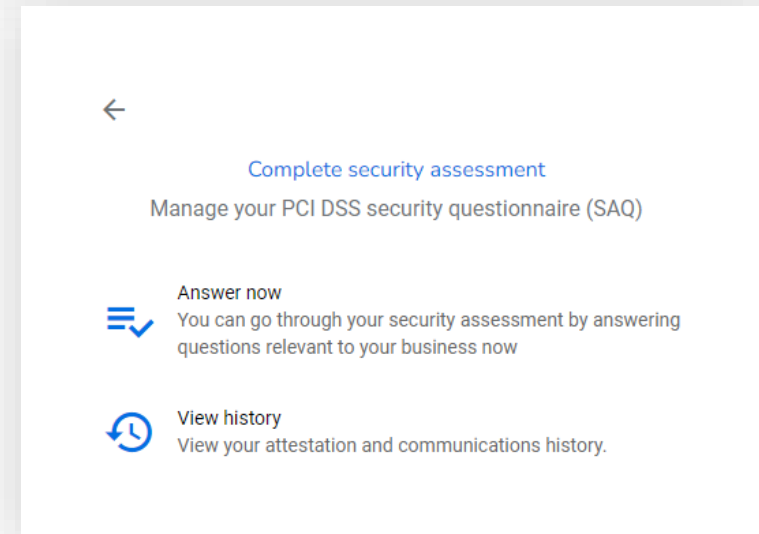
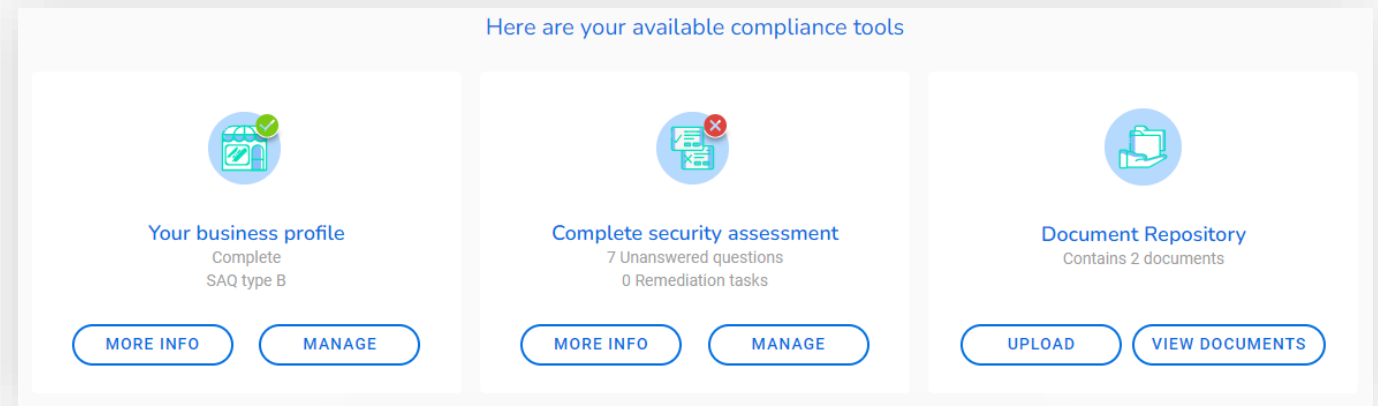
Security Assessment – **Page 22**



Compliance

Security Assessment Questionnaire (SAQ)

- From your dashboard, select 'Manage' on the 'Complete security assessment' widget.
- You will see on your dashboard how many questions you must answer.
 - The number of questions you must answer depends on the business profile assigned to you and is based on your level of risk.



Security Assessment Questionnaire (SAQ)

1

You will be guided through the questions you need to answer to complete your Security Assessment.

2

More information is available via the box underneath to help you understand the question.

The screenshot displays the SecureTrust SAQ interface. At the top, there's a progress bar and a 'Show / Hide / Help' button. Below this, a 'Sections' panel on the right lists: 'Protect Account Data', 'Implement Strong Access Control Measures', 'Maintain an Information Security Policy', and 'Confirm your compliance'. The main content area shows 'Question group 3.5.3' with a 'Help answering this requirement' section. This section includes 'Expected Task' (three bullet points: 'Ensure sensitive data is encrypted', 'Ensure sensitive data is deleted', and 'Observe the secure data deletion process'), 'Applicability Notes' (a paragraph about data retention and deletion), and an 'Information' box with 'Note', 'Purpose', and 'Definitions'.

4

4

The box on the top right shows your progress through the questionnaire. Many of the questions will have been prepopulated for you based on your answers in the profile section. This greatly streamlines the process.

3

Work your way through the questionnaire by answering “Yes”, “No” or “N/A” to the questions.

Security Assessment Questionnaire (SAQ)

- If an answer you provide is against best practice, you may need to further explain your answer or assign yourself a remediation task.
 - You must then 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 assessment questions. However, until these tasks are completed correctly you may not be able to complete your assessment.

3.3.1 

SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.

I have implemented a compensating control



 Remediation task

Reason for non-compliance* 

0 / 1500

Complete documentation* 

0 / 1500

Target date:* 

You will receive a reminder email

Security Assessment Questionnaire (SAQ)

- Once you have answered all your questions correctly, you will need to attest to your compliance. This simply means to confirm the information you have provided is correct.
- You can review all the answers you provided to the questions on this page.
- Once happy, select 'Confirm your Attestation' at the bottom of the screen.

SecureTrust
by vikingCLOUD

MID: Opstest004

Confirm your compliance

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

✓ Your organization information details

Company name: Opstest004 Contact name: Opstest004

Title: Telephone numbers:

Email address: Business address: Opstest004

Opstest004 Opstest004

Opstest004 Ops test

Country: Ireland

✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ B

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

✗ Attestation

✓ Information for Submission.

Based on the results noted in the SAQ B dated Mar 5, 2024, 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 5, 2024:

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

- ✓ Protect Account Data
- ✓ Implement Strong Access Control Measures
- ✓ Maintain an Information Security Policy
- ✗ Confirm your compliance

Next Steps

You've validated your compliance

Your SAQ is valid for one-year.

If scanning is required for your business, a passing scan is required every 90-days.

Your renewal date will be shown on your dashboard.

We will email you to remind you when it's time to revalidate.



Profile



Scanning



Security Assessment



Compliance

You're done for now

1

Your dashboard should have green ticks across the board.

The screenshot shows the SecureTrust dashboard interface. At the top, the logo 'SecureTrust is now vikingCLOUD™' is on the left, and 'MID: Opstest004' with navigation icons is on the right. The main content area features a large 'YOU ARE NOW COMPLIANT' message with a congratulatory note and a coffee cup icon. To the left of this message is a widget labeled 'You're compliant' with a green checkmark icon, a 'Valid until 5 March 2025' date, and a 'DOWNLOAD AOC' button. Below the main message, a section titled 'Here are your available compliance tools' contains three cards: 'Your business profile' (Complete, SAQ type B) with 'MORE INFO' and 'MANAGE' buttons; 'Complete security assessment' (Last attested Mar 5, 2024, 2:26:27 PM) with 'MORE INFO' and 'MANAGE' buttons; and 'Document Repository' (Contains 2 documents) with 'UPLOAD' and 'VIEW DOCUMENTS' buttons.

2

Your revalidation date is displayed in the top left corner widget.



Uploading an Existing Attestation

Already have a valid Attestation of Compliance?

**If applicable under your Acquirer Program.*



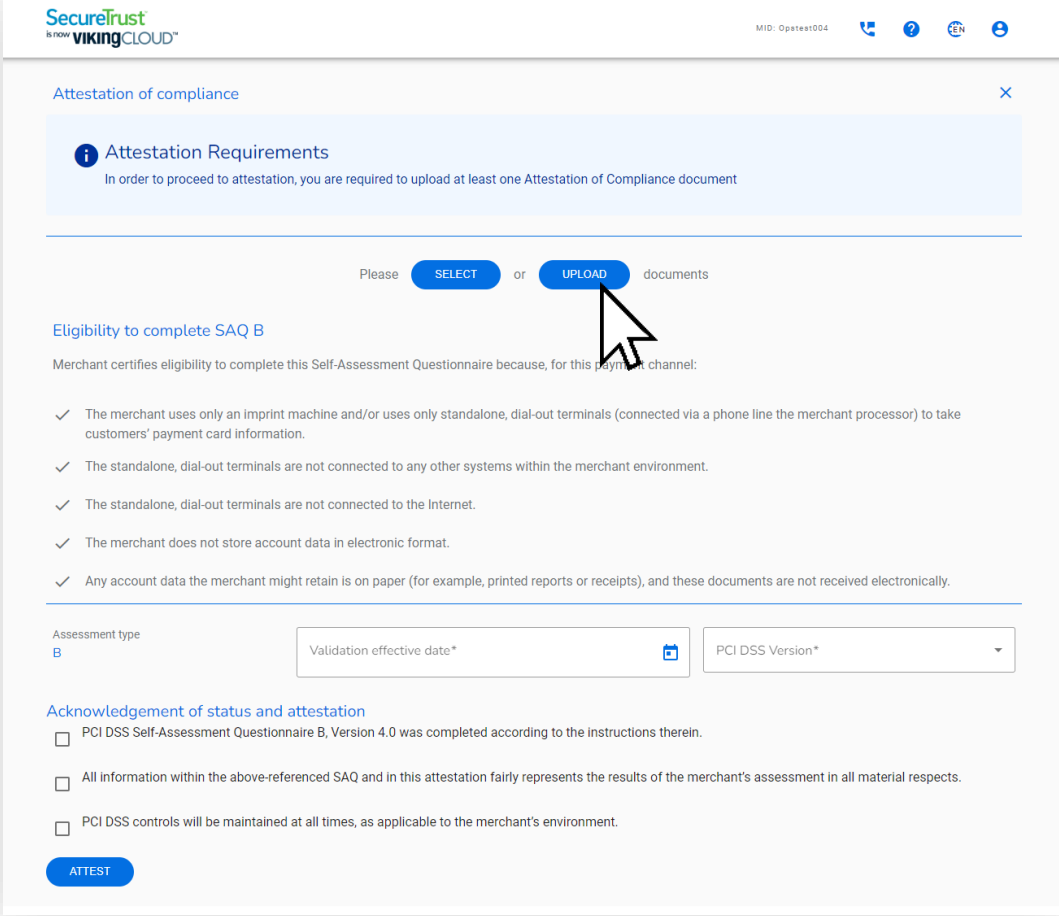
Uploading existing Attestation of Compliance

- If you select that you have an existing attestation of compliance, you will then be asked some questions:
 - The PCI Compliance assessment type of your business. You can find this on your existing certificate.
 - You'll also need to confirm if you use a third party to store or process card payments.
 - You may also have to answer additional questions depending on your previous answers.
- You'll then arrive at your dashboard. The main widget will instruct you to confirm your compliance.
 - Select 'Begin Step' to start.

The image shows two screenshots of the SecureTrust (now vikingCLOUD) interface. The top screenshot is a form titled "Your current valid PCI DSS compliance assessment type". It asks the user to select the PCI DSS compliance assessment type they are submitting. The options are: Self Assessment Questionnaire (SAQ) A, Self Assessment Questionnaire (SAQ) A-EP, Self Assessment Questionnaire (SAQ) B (selected), Self Assessment Questionnaire (SAQ) B-IP, Self Assessment Questionnaire (SAQ) P2PE, Self Assessment Questionnaire (SAQ) C-VT, Self Assessment Questionnaire (SAQ) C, Self Assessment Questionnaire (SAQ) D, Self Assessment Questionnaire (SAQ) D-Service Provider (upload only), and Report on Compliance (upload only). There are "PREVIOUS" and "NEXT" buttons at the bottom. The bottom screenshot shows the dashboard. On the left, there is a widget with a red 'X' icon and the text "You're not compliant. Please complete your remaining compliance tasks." On the right, there is a widget titled "YOUR NEXT STEP" with the text "Confirm you're compliant" and "You have indicated that you are compliant. Please upload your currently valid Attestation of Compliance." Below this text is a blue "BEGIN STEP" button, which is being clicked by a mouse cursor.

Uploading existing Attestation of Compliance

- On the following page you will need to complete some steps:
 - Upload your existing documents.
 - You will need to upload your Attestation of Compliance (AoC) that proves you are currently compliant.
 - Confirm the details, acknowledge your status and attest to your compliance.
- **Instructions on the following pages.**



SecureTrust
is now vikingCLOUD™

MID: Opatest004

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, Version 4.0 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

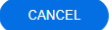
Uploading existing Attestation of Compliance

- Upload your documents
 - Select 'Upload' highlighted on the previous page
 - Select the necessary document(s) from your files
 - Provide details of the document you are uploading and select 'Upload'
 - The document is now attached to your attestation

Please select a file to upload

* Accepted file types: .pdf, .jpg, .jpeg, .doc, .docx, .rtf, .png, .xls, .xlsx. File size limit: 100 MB.



Selected 1/5 files to upload

* Accepted file types: .pdf, .jpg, .jpeg, .doc, .docx, .rtf, .png, .xls, .xlsx. File size limit: 100 MB.



1. TEST_cert_of_compliance.docx 

Document Type* Assessment  Document Date* March 5, 2024 

Additional information 

0 / 1500

PCI DSS Version* 4.0  Assessment type* B-IP  Status* Compliant 



Uploading existing Attestation of Compliance

- Confirm details of your attestation, including:
 - Assessment type.
 - Validation effective date.
 - The version of the PCI DSS to which you are compliant with.
- Confirm by checking the boxes, that you acknowledge a number of conditions in relation to your status and attestation.
- Click 'Attest' to finish. Your validation is now complete.

SecureTrust
vikingCLOUD™

MID: 00000004

File(s) has been uploaded

DISMISS

Attestation of compliance

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

Files to be included in attestation form:

DOCUMENT NAME	DOCUMENT TYPE	DATE UPLOADED	DOCUMENT DATE	
TEST_cert_of_compliance.docx	Assessment	Mar 5, 2024	Mar 5, 2024	×

Items per page: 5 1 - 1 of 1 < >

1 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.

2

Assessment type
B

Validation effective date*

PCI DSS Version*

Acknowledgement of status and attestation

- ☐ PCI DSS Self-Assessment Questionnaire B, Version 4.0 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.

3

ATTEST



Thank you!