

Security Metrics

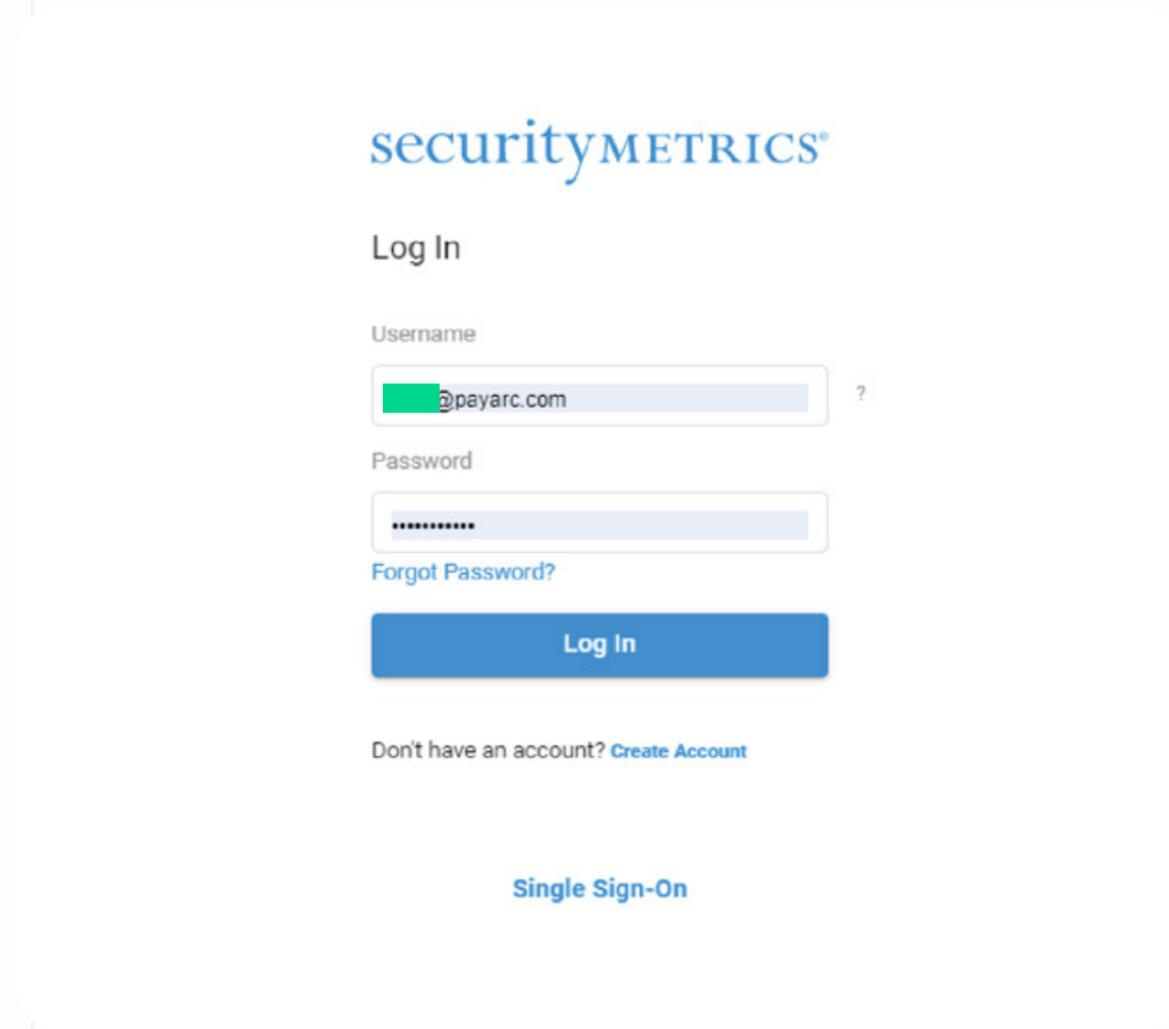
Instructions _____
to become compliant.



CNP accounts: Merchants processing directly through a compliant 3rd party gateway such as NMI, Auth.net, USAEpay, etc.

Login

- Login Link: <https://www.securitymetrics.com/portal/app/ngsm/login>



The screenshot shows the SecurityMetrics login interface. At the top is the SecurityMetrics logo. Below it is the heading "Log In". There are two input fields: "Username" with a value of "[redacted]@payarc.com" and a question mark icon, and "Password" with a masked value of "*****". A "Forgot Password?" link is positioned below the password field. A blue "Log In" button is centered below the fields. At the bottom, there is a link "Don't have an account? Create Account" and a "Single Sign-On" link.

securityMETRICS®

Log In

Username

[redacted]@payarc.com ?

Password

[Forgot Password?](#)

Log In

Don't have an account? [Create Account](#)

[Single Sign-On](#)

User Agreement

- Click “Accept”

SECURITYMETRICS TERMS OF USE AGREEMENT

The following terms and conditions (collectively “Terms of Use Agreement”), are entered into by and between You, the customer (“Customer” or “you”), and SecurityMetrics, Inc., a Utah corporation (“SecurityMetrics”). The Terms of Use Agreement relates to SecurityMetrics’ compliance and data security programs and services, which may include but are not limited to Payment Card Industry Data Security Standard (“PCI DSS”), Health Insurance Portability and Accountability Act (“HIPAA”), Managed Firewall, and other data security and compliance services (collectively “Services”). The Terms of Use Agreement also apply to all content functionality, and services offered or purchased on or through www.securitymetrics.com (the “Website”). By use of any Services or the Website, you accept and agree to all conditions imposed in this Terms of Use Agreement. Note: THIS TERMS OF USE AGREEMENT CONTAINS ARBITRATION, WARRANTIES, AND LIMITATION OF LIABILITY CLAUSES THAT AFFECTS YOUR RIGHTS UNDER THIS TERMS OF USE AGREEMENT WITH RESPECT TO ALL SERVICES.

Services

You may select some or all of the following Services:

PCI Compliance

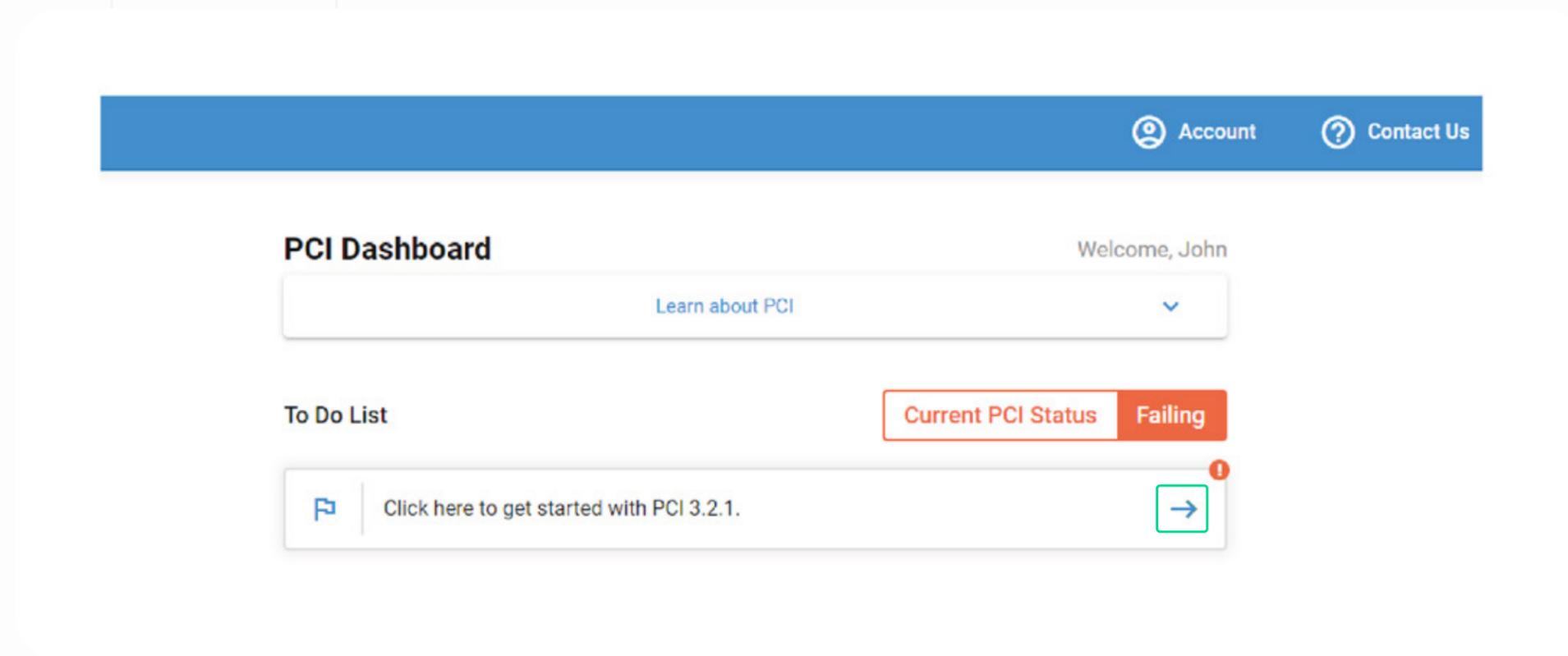
If you have selected service packages that contain PCI Compliance Services, then that package may include, but is not limited to, all or some of the Services listed below.

- Help you determine the scope of the applicable PCI Compliance requirements. You alone are responsible for determining the scope of your PCI Compliance requirements. SecurityMetrics will not be liable for any mistake or error in determining the scope;
- Provide you with a copy of the self-assessment questionnaire determined by the scope determined above and help understanding the questions, if needed;
- Provide vulnerability scanning on IP addresses or domains specified and provided by the Customer; all vulnerability scanning is done in accordance with Warranties and Limitation of Liabilities Sections of this Terms of Use;
- Provide Customer with access to scan results and copies of the self-assessment questionnaire
- Report the status of the self-assessment questionnaire and vulnerability scans via SecurityMetrics website;
- Service Warranty (described below);
- One or more, depending on the invoice, non-exclusive, non-transferable license(s) of PANscan® during the term of this Terms of Use. PANscan® is SecurityMetrics’ software that finds unencrypted credit card numbers on computer systems;
- One or more, depending on the invoice, non-exclusive, non-transferable license(s) of PIIscan® during the term of this Terms of Use. PIIscan® is SecurityMetrics’ software that finds unencrypted personally identifiable information on computer systems;
- SecurityMetrics Mobile, a software application that scans mobile devices for vulnerabilities;
- Seats to PCI Compliance trainings; and
- Technical support.

Accept

Security Metrics Dashboard

- Click on the “arrow” to get started



Partner Confirmation

- Click “Next”

Identify Your Account

You have already been matched to the following bank:

PayArc

Please click Next to continue.

What is this for?

Next

Confirm Account Information

- If anything changed, merchant should update and click “Next”

Customer Information

Company Name *		Company Phone *	
Test CNP account		8772036624	
Address *		City *	
103 Mason Street		Greenwich	
State *	Zip *	Country *	
CT	06830	United States ▼	
		Language Preference *	
		English ▼	

Back

Next

Select Your Processing Method

- Ecom – Auth.net, NMI, USAEpay, ETC
- Check off “eCommerce”
- “I accept payments through a 3rd party”
- Click “Next”

Processing

Please select your methods of processing cardholder data. Check all that apply.

	<input type="checkbox"/> Terminal	I process cardholder data using stand-alone terminals or phones.
	<input type="checkbox"/> Computer	I process cardholder data using a computer.
	<input checked="" type="checkbox"/> eCommerce	I have an eCommerce website.
	<input type="checkbox"/>	I accept payments through my own website
	<input type="checkbox"/>	I accept payments using an I-Frame from a 3rd party source
	<input type="checkbox"/>	I accept payments through a 3rd Party Store (Amazon, Etsy, etc.)
	<input type="checkbox"/>	I accept payments through a 3rd Party Link (Paypal Button, etc.)
	<input checked="" type="checkbox"/>	I accept payments through a 3rd Party Re-Direct (Payment page on another website e.g. authorize.net, sagepay.co.uk, etc.)
	<input type="checkbox"/> Mobile Device	I process cardholder data using a smartphone or tablet.

 If you are a service provider, NOT a merchant, please [click here](#).

[Back](#) [Next](#)

Electronic Storage

- Click “No” – Merchants are not allowed to store CC information, unless using P2PE
- Click “Next”

Electronic Storage [Change previous answers](#)

Do you store cardholder data electronically?
Examples:
Digitally recorded phone calls,
Accepting cardholder data through email or eFax,
Cardholder data stored on a computer,
Your system does not process immediately, but batches out only periodically.

Yes No

Designated SAQ – A 3.2.1

- Click “Activate and Continue”

Congratulations! Based on information you've provided, you have been assigned **SAQ A 3.2.1**.

How can I be sure this is the correct questionnaire?

To ensure you take the correct questionnaire, we need to verify that the following is true:

- You use a PCI compliant third party provider for all of your cardholder transmission and processing
- Any cardholder data that you keep is in paper form (like receipts or copies of receipts)
- You do not store cardholder data electronically

If this doesn't describe your business, click [here](#) or call 801-705-5665 (US) or 0203.014.7820 (UK) 24 hours a day.

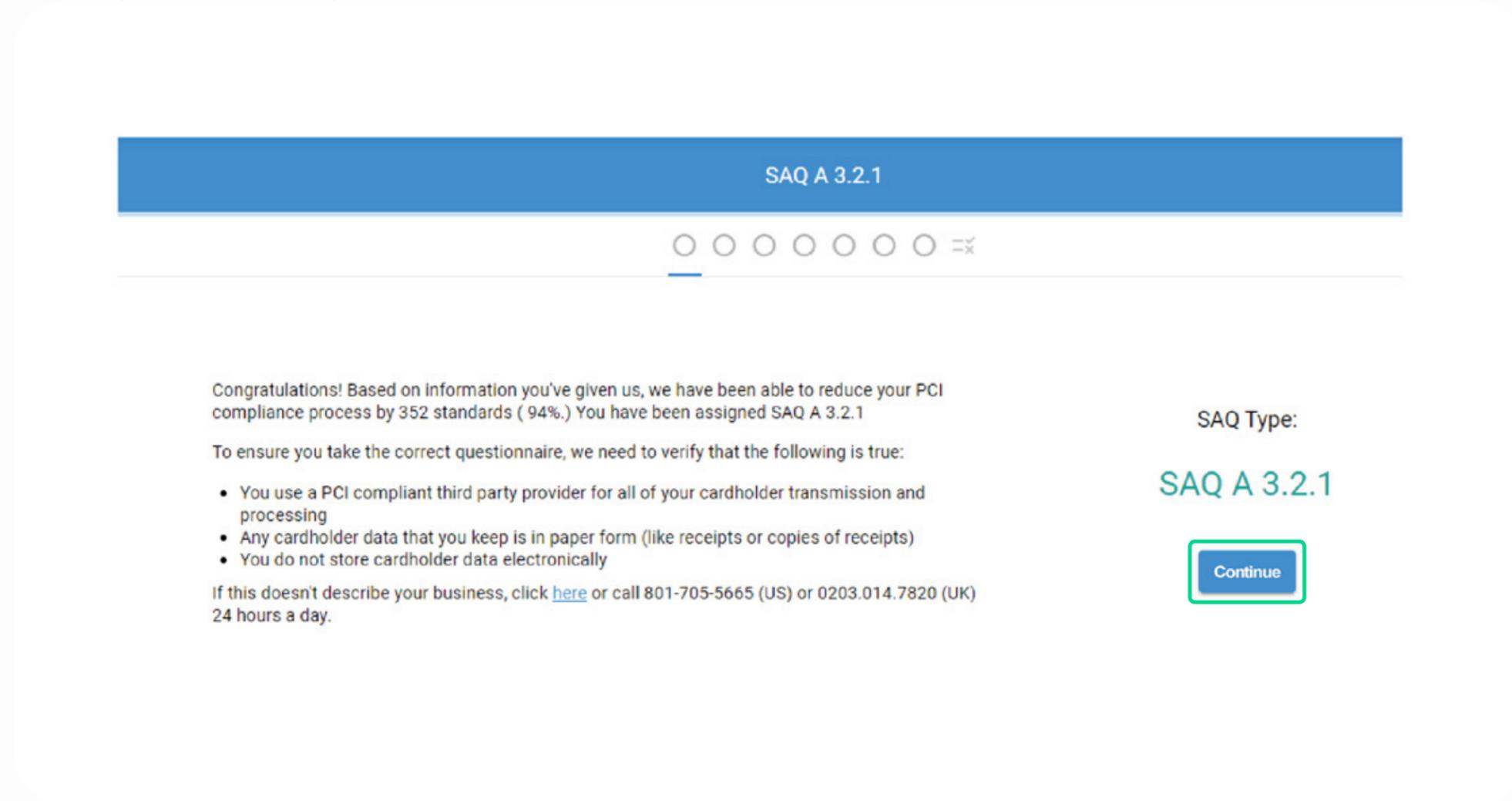
[Back](#)

Questionnaire Type:
SAQ A 3.2.1

[Activate and Continue →](#)

Start Questionnaire

- Click “Continue”



The screenshot shows a questionnaire interface. At the top, a blue header bar contains the text "SAQ A 3.2.1". Below the header is a progress indicator consisting of seven circles, with the first circle filled and underlined. The main content area contains the following text:

Congratulations! Based on information you've given us, we have been able to reduce your PCI compliance process by 352 standards (94%). You have been assigned SAQ A 3.2.1

To ensure you take the correct questionnaire, we need to verify that the following is true:

- You use a PCI compliant third party provider for all of your cardholder transmission and processing
- Any cardholder data that you keep is in paper form (like receipts or copies of receipts)
- You do not store cardholder data electronically

If this doesn't describe your business, click [here](#) or call 801-705-5665 (US) or 0203.014.7820 (UK) 24 hours a day.

SAQ Type:
SAQ A 3.2.1

[Continue](#)

Policy

- Answer Yes or N/A
- If the answer is N/A, you must provide an explanation.
- “This section does not apply to my business” is a valid explanation.
- After answering all the questions, scroll down, and click “Next”

The screenshot shows a web-based assessment form. At the top right, there is a progress indicator with seven circles; the first two are green with checkmarks, and the others are empty. The main heading is 'Policy'. Below it is a paragraph of explanatory text. There are two questions, each with a link to 'Official PCI Text'. The first question is 'Is a list of service providers maintained, including a description of the service(s) provided?' with ID 12.8.1. The second question is 'You should have a written agreement with your providers that acknowledges their responsibility for the cardholder data they possess. Do you have such an agreement?' with ID 12.8.2. Both questions have a green progress bar and a 'YES' button selected.

Policy

The next five standards are regarding service providers. A service provider in this context refers to any organization that you share cardholder data with or that could affect the security of your cardholder data, such as an accountant, managed IT provider, shredding company, attorney or other business partners. Keep in mind that if you do not share cardholder data with service providers and do not allow other organizations to access your systems, you can mark yes to these remaining standards, as you are still compliant.

[Official PCI Text >](#)

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

12.8.1 YES NO N/A

You should have a written agreement with your providers that acknowledges their responsibility for the cardholder data they possess. Do you have such an agreement?

[Official PCI Text >](#)

12.8.2 YES NO N/A

Physical Access

- Answer Yes or N/A
- If the answer is N/A, you must provide an explanation.
“This section does not apply to my business” is a valid explanation.
- After answering all the questions, scroll down, and click “Next”

Physical Access

Is your physical media secure, and is control maintained over moving and storage of that data? Media in this context refers to all paper and electronic media containing cardholder data.

Official PCI Text >

9.5-9.6.a  YES NO N/A

Do controls include the following:

Is the media labeled as “classified” or similar label to indicate the sensitivity of the data?

Official PCI Text >

9.6.1  YES NO N/A

* Please explain why this requirement does not apply to your business:

This section does not apply to my business

Unique IDs

- Answer Yes or N/A
- If the answer is N/A, you must provide an explanation.
“This section does not apply to my business” is a valid explanation.
- After answering all the questions, scroll down, and click “Next”

Unique ID

Are all users assigned a unique ID before allowing them to access system components or cardholder data?

8.1.1



YES

NO

N/A

Is access for any terminated users immediately deactivated or removed?

8.1.3



YES

NO

N/A

Vendor Defaults

- Answer Yes or N/A
- If the answer is N/A, you must provide an explanation.
“This section does not apply to my business” is a valid explanation.
- After answering all the questions, scroll down, and click “Next”

Vendor Defaults

Are vendor-supplied defaults always changed before installing a system on the network?
This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).

2.1.a	<input checked="" type="checkbox"/>	YES	NO	N/A
-------	-------------------------------------	-----	----	-----

Are unnecessary default accounts removed or disabled before installing a system on the network?

2.1.b	<input checked="" type="checkbox"/>	YES	NO	N/A
-------	-------------------------------------	-----	----	-----

[BACK](#) [Restart SAQ](#) [NEXT](#)

Development

- Answer Yes or N/A
- If the answer is N/A, you must provide an explanation.
“This section does not apply to my business” is a valid explanation.
- After answering all the questions, scroll down, and click “Next”

Development

Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?				
6.2.a	<div style="width: 100%; height: 10px; background-color: green;"></div>	YES	NO	N/A

Are critical security patches installed within one month of release? <small>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</small>				
6.2.b	<div style="width: 100%; height: 10px; background-color: green;"></div>	YES	NO	N/A

[BACK](#) [Restart SAQ](#) [NEXT](#)

Choosing Your 3rd Party Provider

- Under webhost, type in the name of your gateway provider.
If no results were found after entering the name, Ex: “ NMI”
- Then click “Add”
- Click “Next”

How do you accept cards?

SAQ A 3.2.1

The following are different possible methods of processing cardholder data. Please select only the methods that you use.

Merchants are responsible to ensure the PCI compliance of any third party providers that capture, store or transmit cardholder data on their behalf. We recommend you obtain PCI compliance documentation from your provider. The scope of this SAQ does not include validation of your providers' compliance.

WARNING:
Using a non-compliant provider could result in significant financial penalties to your business in the event of a data compromise.

Please enter the details of your card processing methods. At least one third party provider must be filled out to proceed.

Web Host ⓘ

NMI Add

No Results Found

Click here to add providers

BACK Restart SAQ NEXT

Confirm Your Assessment

- Click “I Agree”

SAQ A 3.2.1

✓ ✓ ✓ ✓ ✓ ✓ ✓ ☰

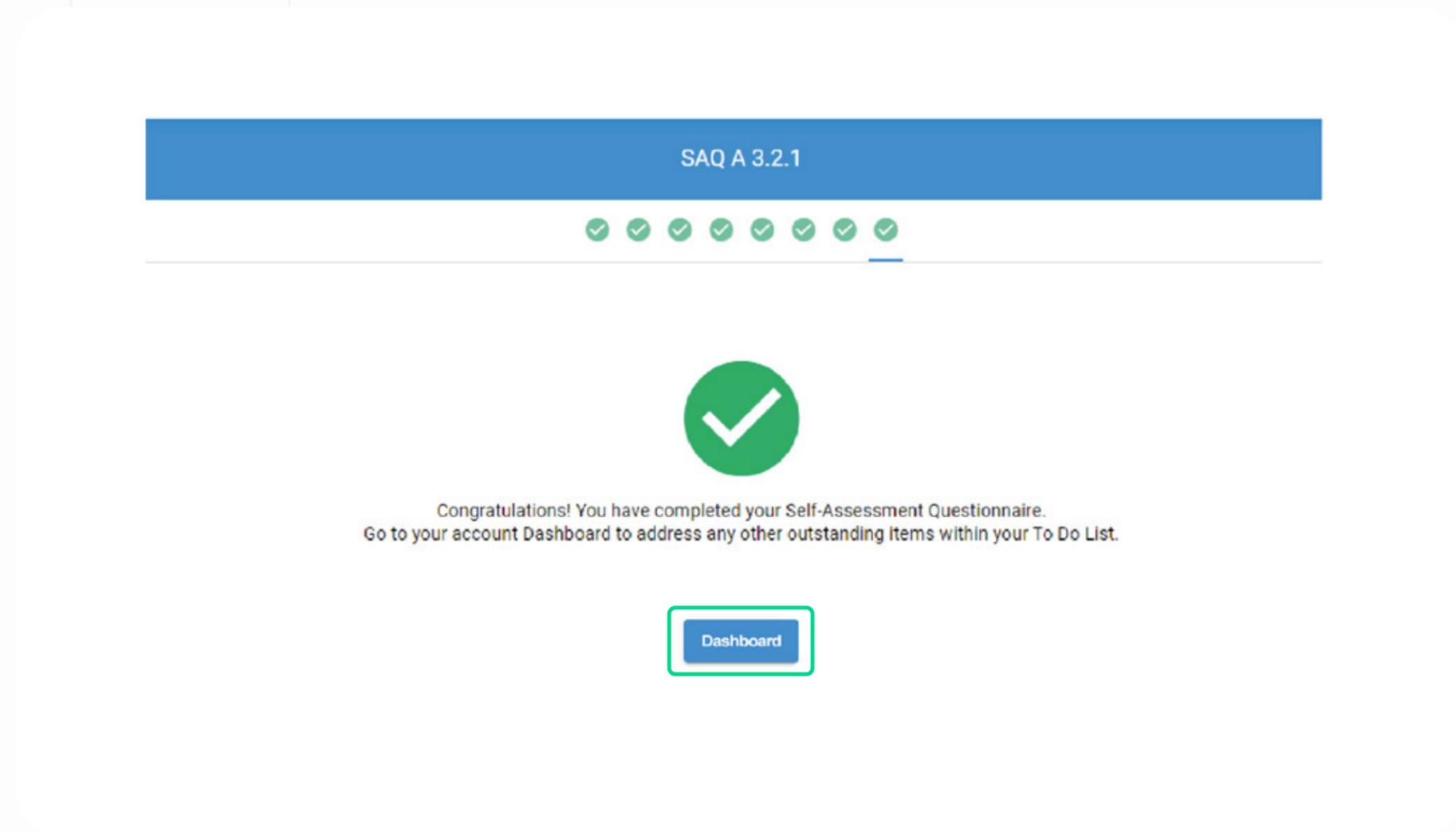
Confirm below to complete your Assessment.

I verify that the following is true:

- PCI Self-Assessment Questionnaire A version 3.2.1, was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

PCI-SAQ Compliance Confirmation

- To go back to the home screen, click “Dashboard”



How to retrieve your PCI Certificate & SAQ?

- From the home screen, Click “Menu” > “Reports”

The screenshot displays the SecurityMetrics web application interface. At the top, there is a blue navigation bar with the SecurityMetrics logo on the left and links for Account, Contact Us, and Log Out on the right. A left-hand sidebar menu contains options for Dashboard, Self-Assessment Questionnaire, Reports (highlighted with a green box), and PCI Policies. The main content area is divided into two sections: PCI Data Security Standard (DSS) Reports and PCI Data Security Evaluation (DSE) Reports. Each section contains a list of report options with icons, titles, and descriptions. In the DSS section, 'Merchant PCI Certificate (Download PDF)' and 'Self-Assessment Questionnaire (SAQ)' are highlighted with green boxes. In the DSE section, 'Evaluation Form' and 'Confirmation of Status' are listed.

PCI Data Security Standard (DSS) Reports		
	Send Summary Compliance Report	Send a report of PCI Compliance to your acquirer, franchisor, etc.
	Merchant PCI Certificate (Download PDF)	Generate a 'suitable for framing' certificate of PCI Compliance. (html or pdf)
	Attestation of Compliance	SecurityMetrics populates the Attestation of Compliance with compliance information when applicable.
	Self-Assessment Questionnaire (SAQ)	Download a pdf file of your Self-Assessment Questionnaire. (pdf)
	Prioritized Approach	Download a report of your progress in a prioritized format.
	ASV Reports	Download ASV Scan Report Attestation of Scan Compliance, ASV Scan Report Executive Summary, ASV Scan Report Vulnerability Details, and the ASV Feedback Form.

PCI Data Security Evaluation (DSE) Reports		
	Evaluation Form	Download a pdf file of your DSE Evaluation Form. (pdf)
	Confirmation of Status	Generate a Data Security Essentials Evaluation Confirmation of Status.

Thank You For Becoming PCI-DSS Compliant!

* SAQ Valid for 1 Year