Payment Card Industry
Data Security Standard

Self-Assessment Questionnaire A and Attestation of Compliance

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: January 2025

Document Changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1*.
July 2015	3.1	1.1	Updated version numbering to align with other SAQs.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2.* Requirements added from PCI DSS v3.2 Requirements 2, 8, and 12.
January 2017	3.2	1.1	Updated Document Changes to clarify requirements added in the April 2016 update. Added note to Before You Begin section to clarify intent of inclusion of PCI DSS Requirements 2 and 8.
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1.* Added Requirement 6.2 from PCI DSS v3.2.1.
April 2022	4.0		Updated to align with PCI DSS v4.0. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.2.1 to 4.0. Rearranged, retitled, and expanded information in the "Completing the Self-Assessment Questionnaire" section (previously titled "Before You Begin"). Aligned content in Sections 1 and 3 of Attestation of Compliance (AOC) with PCI DSS v4.0 Report on Compliance AOC. Added PCI DSS v4.0 requirements. Added appendices to support new reporting responses.
December 2022	4.0	1	Removed "In Place with Remediation" as a reporting option from Requirement Responses table, Attestation of Compliance (AOC) Part 2g, SAQ Section 2 Response column, and AOC Section 3. Also removed former Appendix C. Added "In Place with CCW" to AOC Section 3. Added guidance for responding to future-dated requirements. Clarified note under Eligibility Criteria on page iv that addresses applicability of Requirements 2, 6, 8, and 11 to e-commerce merchants. Clarified notes that address applicability to e-commerce merchants for Requirements 6.4.3, 8, 11 and 11.6.1. Added minor clarifications and addressed typographical errors.
July 2023	4.0	2	Address typographical error in Requirement 11.6.1 SAQ Completion Guidance - changed "merchant's payment page/form" to "TPSP's/payment processor's payment page/form".
October 2024	4.0.1		Updated to align with PCI DSS v4.0.1. For details of PCI DSS changes, see *PCI DSS Summary of Changes from PCI DSS Version 4.0 to 4.0.1.* Updated an SAQ Eligibility Criteria that the merchant has confirmed "their TPSP(s) are PCI DSS compliant for the services used by the merchant" rather than that the merchant has reviewed the TPSP(s)' AOCs. Added ASV Resource Guide to section "Additional PCI SSC Resources." Added SAQ Completion Guidance for Requirement 6.4.3. Added Requirement 12.3.1, as the completion of this requirement is specified in Requirement 11.6.1.
January 2025	4.0.1	1	Removed Requirements 6.4.3, 11.6.1, and 12.3.1 and added an Eligibility Criteria for merchants to confirm that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s).

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Contents

Document Changes i

Completing the Self-Assessment Questionnaire iii

Merchant Eligibility Criteria for Self-Assessment Questionnaire A iii

PCI DSS Self-Assessment Completion Steps iv

Expected Testing iv

Requirement Responses v

Additional PCI SSC Resources vii

Section 1: Assessment Information 1

Section 2: Self-Assessment Questionnaire A 6

Build and Maintain a Secure Network and Systems 6

Requirement 2: Apply Secure Configurations to All System Components 6

Protect Account Data 7

Requirement 3: Protect Stored Account Data 7

Maintain a Vulnerability Management Program 10

Requirement 6: Develop and Maintain Secure Systems and Software 10

Implement Strong Access Control Measures 12

Requirement 8: Identify Users and Authenticate Access to System Components 12

Requirement 9: Restrict Physical Access to Cardholder Data 16

Requirement 11: Test Security of Systems and Networks Regularly 18

Maintain an Information Security Policy 20

Requirement 12: Support Information Security with Organizational Policies and Programs 20

Appendix A: Additional PCI DSS Requirements 24

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers 24

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections 24

Appendix A3: Designated Entities Supplemental Validation (DESV) 24

Appendix B: Compensating Controls Worksheet 25

Appendix C: Explanation of Requirements Noted as Not Applicable 26

Appendix D: Explanation of Requirements Noted as Not Tested 27

Section 3: Validation and Attestation Details 28

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Completing the Self-Assessment Questionnaire

Merchant Eligibility Criteria for Self-Assessment Questionnaire A

Self-Assessment Questionnaire (SAQ) A includes only those PCI DSS requirements applicable to merchants with account data functions completely outsourced to PCI DSS validated and compliant third parties, where the merchant retains only paper reports or receipts with account data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present) and do not store, process, or transmit any account data in electronic format on their systems or premises.

This SAQ is not applicable to face-to-face channels.

This SAQ is not applicable to service providers.

SAQ A merchants confirm that, for this payment channel:

- The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP)/payment processor;
- The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
- The merchant has confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.
- The merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s).

This SAQ includes only those requirements that apply to a specific type of merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to the cardholder data environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for the merchant's environment.

Note: *For this SAQ, PCI DSS Requirements that address the protection of computer systems (for example, Requirements 2, 6, 8, and 11) AND requirements that refer to the "cardholder data environment" apply to the following e-commerce merchants:*

- *Those with a webpage(s) that redirects customers from their website to a TPSP/payment processor for payment processing, and specifically to the merchant webpage upon which the redirection mechanism is located.*
- *Those with a webpage(s) that includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frames or iframes), and specifically to the merchant webpage that includes the embedded payment page/form.*

These PCI DSS requirements are applicable because the above merchant webpages impact how the account data is transmitted, even though the webpages themselves do not receive account data.

Mail order/telephone order (MOTO) or e-commerce merchants that have completely outsourced all operations (where there is no redirection mechanism from the merchant to the TPSP/payment processor and no embedded payment form from a TPSP/payment processor) and therefore do not have any systems in scope for this SAQ, would consider these requirements to be "not applicable." Refer to guidance on the following pages for how to report requirements that are not applicable.

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of cardholder data and/or sensitive authentication data. Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

Refer to PCI DSS Section 2, *PCI DSS Applicability Information*, for further details.

PCI DSS Self-Assessment Completion Steps

1. Confirm by review of the eligibility criteria in this SAQ and the *Self-Assessment Questionnaire Instructions and Guidelines* document on the PCI SSC website that this is the correct SAQ for the merchant's environment.
2. Confirm that the merchant environment is properly scoped.
3. Assess the environment for compliance with PCI DSS requirements.
4. Complete all sections of this document:
   - Section 1: Assessment Information (Parts 1 & 2 of the Attestation of Compliance (AOC) – Contact Information and Executive Summary).
   - Section 2 – Self-Assessment Questionnaire A.
   - Section 3: Validation and Attestation Details (Parts 3 & 4 of the AOC – PCI DSS Validation and Action Plan for Non-Compliant Requirements (if Part 4 is applicable)).
5. Submit the SAQ and AOC, along with any other requested documentation—such as ASV scan reports—to the requesting organization (those organizations that manage compliance programs such as payment brands and acquirers).

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in PCI DSS and provide a high-level description of the types of testing activities that a merchant is expected to perform to verify that a requirement has been met.

The intent behind each testing method is described as follows:

- Examine: The merchant critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- Observe: The merchant watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, environmental conditions, and physical controls.

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

- Interview: The merchant converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

The testing methods are intended to allow the merchant to demonstrate how it has met a requirement. The specific items to be examined or observed and personnel to be interviewed should be appropriate for both the requirement being assessed and the merchant's particular implementation.

Full details of testing procedures for each requirement can be found in PCI DSS.

Requirement Responses

For each requirement item, there is a choice of responses to indicate the merchant's status regarding that requirement. ***Only one response should be selected for each requirement item.***

A description of the meaning for each response and when to use each response is provided in the table below:

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.
In Place with CCW (Compensating Controls Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in PCI DSS in Appendices B and C.
Not Applicable	The requirement does not apply to the merchant's environment. (See "Guidance for Not Applicable Requirements" below for examples.) All responses in this column require a supporting explanation in Appendix C of this SAQ.
Not Tested	*This response is not applicable to, and not included as an option for, this SAQ.* *This SAQ was created for a specific type of environment based on how the merchant stores, processes, and/or transmits account data and defines the specific PCI DSS requirements that apply for this environment. Consequently, all requirements in this SAQ must be tested.*
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before the merchant can confirm they are in place. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted. This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance).

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Guidance for Not Applicable Requirements

If any requirements do not apply to the merchant's environment, select the Not Applicable option for that specific requirement. For example, in this SAQ, requirements for securing all media with cardholder data (Requirements 9.4.1 - 9.4.6) only apply if a merchant stores paper media with cardholder data; if paper media is not stored, the merchant can select Not Applicable for those requirements.

For each response where Not Applicable is selected in this SAQ, complete *Appendix C: Explanation of Requirements Noted as Not Applicable*.

Guidance for Responding to Future Dated Requirements

In Section 2 below, each PCI DSS requirement or bullet with an extended implementation period includes the following note: "*This requirement [or bullet] is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*"

These new requirements are not required to be included in a PCI DSS assessment until the future date has passed. Prior to that future date, any requirements with an extended implementation date that have not been implemented by the merchant may be marked as Not Applicable and documented in *Appendix C: Explanation of Requirements Noted as Not Applicable*.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, select Not in Place for that requirement and complete the relevant attestation in Section 3, Part 3 of this SAQ.

Note: *A legal exception is a legal restriction due to a local or regional law, regulation, or regulatory requirement, where meeting a PCI DSS requirement would violate that law, regulation, or regulatory requirement.*

Contractual obligations or legal advice are ***not*** *legal restrictions.*

Use of the Customized Approach

SAQs cannot be used to document use of the Customized Approach to meet PCI DSS requirements. For this reason, the Customized Approach Objectives are not included in SAQs. Entities wishing to validate using the Customized Approach may be able to use the PCI DSS Report on Compliance (ROC) Template to document the results of their assessment.

Use of the Customized Approach is not supported in SAQs.

The use of the customized approach may be regulated by organizations that manage compliance programs, such as payment brands and acquirers. Questions about use of a customized approach should always be referred to those organizations. This includes whether an entity that is eligible for an SAQ may instead complete a ROC to use a customized approach, and whether an entity is required to use a QSA, or may use an ISA, to complete an assessment using the customized approach. Information about the use of the Customized Approach can be found in Appendices D and E of PCI DSS.

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Additional PCI SSC Resources

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided below to assist with the assessment process.

Resource	Includes:
PCI Data Security Standard Requirements and Testing Procedures (PCI DSS)	▪ Guidance on Scoping ▪ Guidance on the intent of all PCI DSS Requirements ▪ Details of testing procedures ▪ Guidance on Compensating Controls ▪ Appendix G: Glossary of Terms, Abbreviations, and Acronyms
SAQ Instructions and Guidelines	▪ Information about all SAQs and their eligibility criteria ▪ How to determine which SAQ is right for your organization
Frequently Asked Questions (FAQs)	▪ Guidance and information about SAQs.
Online PCI DSS Glossary	▪ PCI DSS Terms, Abbreviations, and Acronyms
Information Supplements and Guidelines	▪ Guidance on a variety of PCI DSS topics including: – *Understanding PCI DSS Scoping and Network Segmentation* – *Third-Party Security Assurance* – *Multi-Factor Authentication Guidance* – *Best Practices for Maintaining PCI DSS Compliance*
Getting Started with PCI	▪ Resources for smaller merchants including: – *Guide to Safe Payments* – *Common Payment Systems* – *Questions to Ask Your Vendors* – *Glossary of Payment and Information Security Terms* – *PCI Firewall Basics* – *ASV Resource Guide*

These and other resources can be found on the PCI SSC website *(www.pcisecuritystandards.org)*.

Organizations are encouraged to review PCI DSS and other supporting documents before beginning an assessment.

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures.* Complete all sections. The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

Part 1. Contact Information	
Part 1a. Assessed Merchant	
Company name:	INN Partners, LC
DBA (doing business as):	BLOX Digital
Company mailing address:	4600 E 53rd St, Davenport, IA 52807
Company main website:	https://www.bloxdigital.com/
Company contact name:	Christopher Murley
Company contact title:	Director of Network Operations
Contact phone number:	(309) 743-0814
Contact e-mail address:	cmurley@bloxdigital.com
Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	Not Applicable
Company mailing address:	Not Applicable
Company website:	Not Applicable
Lead Assessor Name:	Not Applicable
Assessor phone number:	Not Applicable
Assessor e-mail address:	Not Applicable
Assessor certificate number:	Not Applicable

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):

Indicate all payment channels used by the business that are included in this assessment.

☐ Mail order/telephone order (MOTO)

☒ E-Commerce

☐ Card-present

Are any payment channels not included in this assessment? If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.	☐ Yes ☒ No

Note: *If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.*

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes, and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data
E-Commerce	Cards are processed by a third-party only, via iframes

Part 2c. Description of Payment Card Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	No direct credit card processing, transmitting, or storing is done
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☒ Yes ☐ No

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2. Executive Summary *(continued)*

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers, and mail rooms) in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Lumen Datacenter	1	Chicago, IL USA
Lumen Datacenter	1	Weehawken, NJ USA

Part 2e. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions♦?

☐ Yes ☒ No

Provide the following information regarding each item the merchant uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

♦ For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions, and Mobile Payments on COTS (MPoC) products.

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

Does the merchant have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the merchant's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	☒ Yes ☐ No
• Manage system components included in the scope of the merchant's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	☐ Yes ☒ No
• Could impact the security of the merchant's CDE (for example, vendors providing support via remote access, and/or bespoke software developers)	☐ Yes ☒ No

If Yes:

Name of service provider:	**Description of service(s) provided:**
Spreedly	Card processing provider using iFrames

Note: *Requirement 12.8 applies to all entities in this list.*

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement *	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*			
	In Place	In Place with CCW	Not Applicable	Not in Place
Requirement 2:	☒	☐	☐	☐
Requirement 3:	☒	☐	☐	☐
Requirement 6:	☒	☐	☐	☐
Requirement 8:	☒	☐	☐	☐
Requirement 9:	☐	☐	☒	☐
Requirement 11:	☒	☐	☐	☐
Requirement 12:	☒	☐	☐	☐

** PCI DSS Requirements indicated above refer to the requirements in Section 2 of this SAQ.*

Part 2h. Eligibility to Complete SAQ A

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

☒	The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transaction.
☒	All processing of account data is entirely outsourced to a PCI DSS compliant third-party service provider (TPSP)/payment processor.
☒	The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions.
☒	The merchant has confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant.
☒	Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.
Additionally, for e-commerce channels, merchant certifies:	
☒	All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.
☒	The merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s).

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix B: Compensating Controls Worksheet

This Appendix must be completed to define compensating controls for any requirement where In Place with CCW was selected.

Note: *Only entities that have a legitimate and documented technological or business constraint can consider the use of compensating controls to achieve compliance.*

Refer to Appendices B and C in PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	
2. Definition of Compensating Controls	Define the compensating controls: explain how they address the objectives of the original control and the increased risk, if any.	
3. Objective	Define the objective of the original control.	
	Identify the objective met by the compensating control. ***Note:*** *This can be, but is not required to be, the stated Customized Approach Objective listed for this requirement in PCI DSS.*	
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix C: Explanation of Requirements Noted as Not Applicable

This Appendix must be completed for each requirement where Not Applicable was selected.

Requirement	Reason Requirement is Not Applicable
Example:	
Requirement 3.5.1	*Account data is never stored electronically*
Requirement 9	Credit card data is never captured or stored

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix D: Explanation of Requirements Noted as Not Tested

This Appendix is not used for SAQ A merchant assessments.

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ A (Section 2), dated (Self-assessment completion date *YYYY-MM-DD*).

Based on the results documented in the SAQ A noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

Select one:

☒	**Compliant:** All sections of the PCI DSS SAQ are complete and all requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Merchant Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Merchant Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: *YYYY-MM-DD* A merchant submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted *before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Merchant Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

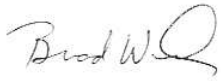
Part 3a. Merchant Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	*PCI DSS Self-Assessment Questionnaire A, Version 4.0.1,* 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.

Part 3b. Merchant Attestation



Signature of Merchant Executive Officer ↑	*Date: 2026-09-15*
Merchant Executive Officer Name: **Brad Ward**	*Title:* **CEO, BLOX Digital**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	☐ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	*Date: YYYY-MM-DD*
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date: YYYY-MM-DD*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the merchant expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	

** PCI DSS Requirements indicated above refer to the requirements in Section 2 of this SAQ.*

Note: *The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance-accepting organization to ensure that this form is acceptable in its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.*

© 2006–2025 PCI Security Standards Council, LLC. All Rights Reserved.