



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 <i>PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1</i> .
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 <i>PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2</i> . 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 <i>PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1</i> . 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 <i>PCI DSS – Summary of Changes from PCI DSS Version 3.2.1 to 4.0</i> . 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, 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 <i>PCI DSS Summary of Changes from PCI DSS Version 4.0 to 4.0.1</i> . 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).

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
<i>Requirement 2: Apply Secure Configurations to All System Components</i>	<i>6</i>
Protect Account Data	7
<i>Requirement 3: Protect Stored Account Data</i>	<i>7</i>
Maintain a Vulnerability Management Program	10
<i>Requirement 6: Develop and Maintain Secure Systems and Software</i>	<i>10</i>
Implement Strong Access Control Measures	12
<i>Requirement 8: Identify Users and Authenticate Access to System Components</i>	<i>12</i>
<i>Requirement 9: Restrict Physical Access to Cardholder Data</i>	<i>16</i>
<i>Requirement 11: Test Security of Systems and Networks Regularly</i>	<i>18</i>
Maintain an Information Security Policy.....	20
<i>Requirement 12: Support Information Security with Organizational Policies and Programs</i>	<i>20</i>
Appendix A: Additional PCI DSS Requirements	24
<i>Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers</i>	<i>24</i>
<i>Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections.....</i>	<i>24</i>
<i>Appendix A3: Designated Entities Supplemental Validation (DESV)</i>	<i>24</i>
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

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.

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.

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: - Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. - Materials are stored in secure storage containers prior to destruction.	- Examine the periodic media destruction policy. - Observe processes. - Interview personnel. - Observe storage containers.	☐	☐	☒	☐
		Applicability Notes				
		These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.				
SAQ Completion Guidance: Selection of any of the In Place responses for Requirements at 9.4 means that the merchant securely stores any paper media with account data, for example by storing the paper in a locked drawer, cabinet, or safe, and that the merchant destroys such paper when no longer needed for business purposes. This includes a written document or policy for employees, so they know how to secure paper with account data and how to destroy the paper when no longer needed. If the merchant never stores any paper with account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.						

Requirement 11: Test Security of Systems and Networks Regularly

Note: For SAQ A, Requirement 11 applies to merchant server(s) with a webpage that either 1) redirects customers from the merchant website to a TPSP/payment processor for payment processing (for example, with a URL redirect) or 2) includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frames or iframes).

PCI DSS Requirement	Expected Testing	Response [♦] (Check one response for each requirement)		
		In Place	In Place with CCW	Not Applicable
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.				
11.3.2	External vulnerability scans are performed as follows: • At least once every three months. • By PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and <i>ASV Program Guide</i> requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the <i>ASV Program Guide</i> requirements for a passing scan.	☒	☐	☐
Applicability Notes For the initial PCI DSS assessment against this requirement, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred. ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer. Refer to the <i>ASV Program Guide</i> published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.				

♦ Refer to the "Requirement Responses" section (page v) for information about these response options.

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)		
			In Place	In Place with CCW	Not Applicable
11.3.2.1	External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	• Examine change control documentation. • Interview personnel. • Examine external scan, and as applicable rescan reports.	☒	☐	☐

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

Note: Requirement 12 specifies that merchants have information security policies for their personnel, but these policies can be as simple or complex as needed for the size and complexity of the merchant's operations. The policy document must be provided to all personnel, so they are aware of their responsibilities for protecting payment terminals, any paper documents with cardholder data and/or sensitive authentication data, etc. If a merchant has no employees, then it is expected that the merchant understands and acknowledges their responsibility for security within their store(s).

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.						
12.8.1	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	• Examine policies and procedures. • Examine list of TPSPs.	☒	☐	☐	☐
Applicability Notes						
The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.						

♦ Refer to the "Requirement Responses" section (page v) for information about these response options.

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8.2	Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data.	• Examine policies and procedures. • Examine written agreements with TPSPs.	☒	☐	☐	☐
Applicability Notes						
The exact wording of an agreement will depend on the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement. The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data. Evidence that a TPSP is meeting PCI DSS requirements (is not the same as a written acknowledgment specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment.						
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	• Examine policies and procedures. • Examine evidence. • Interview responsible personnel.	☒	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)		
			In Place	In Place with CCW	Not in Place
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☒	☐	☐
Applicability Notes					
Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.					
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☒	☐	☐
SAQ Completion Guidance: <i>Selection of any of the In Place responses for requirements at 12.8.1 through 12.8.5 means that the merchant has a list of, and agreements with, service providers they share account data with or that could impact the security of the merchant's cardholder data environment. For example, such agreements would be applicable if a merchant uses a document-retention company to store paper documents that include account data or if a merchant's vendor accesses merchant systems remotely to perform maintenance.</i>					

PCI DSS Requirement		Expected Testing	Response♦ <i>(Check one response for each requirement)</i>			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.						
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	• Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents.	☒	☐	☐	☐
SAQ Completion Guidance: Selection of any of the In Place responses for Requirement 12.10.1 means that the merchant has documented an incident response and escalation plan to be used for emergencies, consistent with the size and complexity of the merchant's operations. For example, such a plan could be a simple document posted in the back office that lists who to call in the event of various situations with an annual review to confirm it is still accurate, but could extend all the way to a full incident response plan including backup "hot site" facilities and thorough annual testing. This plan should be readily available to all personnel as a resource in an emergency.						

Appendix A: Additional PCI DSS Requirements

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

This Appendix is not used for merchant assessments.

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

This Appendix is not used for SAQ A merchant assessments.

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting and consult with the applicable payment brand and/or acquirer for submission procedures.

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.	

Appendix D: Explanation of Requirements Noted as Not Tested

This Appendix is not used for SAQ A merchant assessments.

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 (<i>Merchant Company Name</i>) 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 (<i>Merchant Company Name</i>) 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 <i>before completing Part 4</i>.								
☐	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 (<i>Merchant Company Name</i>) 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. <i>If selected, complete the following:</i> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								

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:

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/.