



Payment Card Industry Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers

For use with PCI DSS Version 4.0.1

Publication Date: October 2024



Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the entity's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*. Complete all sections: The entity 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.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Entity	
Company name:	Zscaler, Inc.
DBA (doing business as):	Not applicable.
Company mailing address:	120 Holger Way, San Jose, CA 95134
Company main website:	www.zscaler.com
Company contact name:	Kumar Selvaraj
Company contact title:	Vice President, Security and Compliance
Contact phone number:	(408) 533-0288
Contact e-mail address:	kselvaraj@zscaler.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:	Schellman Compliance, LLC
Company mailing address:	4010 W Boy Scout Boulevard, Suite 600, Tampa, FL 33607
Company website:	https://www.schellman.com/services/pci-compliance
Lead Assessor Name:	Salvatore Butera
Assessor phone number:	866.254.0000 x684
Assessor e-mail address:	salvatore.butera@schellman.com
Assessor certificate number:	QSA Certificate # 206-271



Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (select all that apply):

Name of service(s) assessed: Zscaler Cloud Service

Type of service(s) assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☒ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☒ Other Hosting (specify):
Zero trust SaaS platform

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):
Not applicable.

Payment Processing:

- ☐ POI / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):
Not applicable.

☐ Account Management

☐ Fraud and Chargeback

☐ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☐ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify): Not applicable.

Note: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.



Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (select all that apply):

Name of service(s) not assessed: Not applicable.

Type of service(s) not assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☐ Other Hosting (specify):
Not applicable.

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):
Not applicable.

Payment Processing:

- ☐ POI / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):
Not applicable.

☐ Account Management

☐ Fraud and Chargeback

☐ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☐ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify): Not applicable.

Provide a brief explanation why any checked services were not included in the assessment:

Not applicable.

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.

Zscaler is a cloud-native cybersecurity company that provides secure access to the internet and private applications for organizations. Due to the nature of its services, Zscaler does not store, process, or transmit cardholder data.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.

Zscaler provides secure access to the internet and private applications for organizations, regardless of where their users are located. Rather than relying on traditional hardware-based security systems that route traffic through a central office, Zscaler operates entirely in the cloud. It inspects and filters internet traffic in real time to block threats, prevent data loss, and enforce security policies. Zscaler's services could be used to protect customers managed cardholder data environments.



Describe system components that could impact the security of account data.	<p>The Zscaler Cloud Platform for this review consists of the following products: Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA).</p> <p>Zscaler operates a globally distributed cloud capable of providing inline inspection that offers a full range of enterprise network security services. Zscaler designed a purpose-built three-tier architecture starting with Zscaler’s proprietary operating system (ZOS).</p> <p>Zscaler’s cloud is distributed across more than 150 data centers globally. The platform is designed to be resilient, redundant, and high performing.</p> <p>The platform modules are split into the control plane (Zscaler Central Authority), the enforcement plane (Zscaler Service Edges) and the logging and statistics plane (Zscaler log Servers).</p>
--	---



Part 2. Executive Summary (continued)

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.

The scope of this assessment includes the Zscaler Cloud platform, which provides cloud-delivered security services to customer environments and applications. Zscaler acts as a secure intermediary between users and the internet or internal applications, delivering its services. These services are designed to inspect, filter, and control traffic in real time, ensuring secure access and compliance with customer defined security policies. This assessment evaluates the controls and processes in place within the Zscaler Cloud that could be used by customers for protection of their CDE and the support of PCI DSS compliance for Zscaler's customers.

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

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities—for example, 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)
Data Centers	150	Americas <ul style="list-style-type: none">▪ Vancaouver, Canada▪ Seattle, United States▪ San Francisco, United States▪ Los Angeles, United States▪ Denver, United States▪ Dallas, United States▪ Miami, United States▪ Atlanta, United States▪ Chicago, United States▪ Washington DC, United States▪ Toronto, Canada▪ New York, United States▪ Boston, United States▪ Montreal, Canada▪ Nuevo Laredo, Mexico▪ Mexico, Mexico▪ Bogota, Colombia▪ Rio de Janeiro, Brazil



Part 2d. In-Scope Locations/Facilities

		<ul style="list-style-type: none">Sao Paulo, BrazilSantiago, ChileBuenos Aires, Argentina
		<div>EMEA (Europe, Middle East, and Africa)</div> <ul style="list-style-type: none">Lisbon, PortugalMadrid, SpainMarseille, FranceMilan, ItalyMunich, GermanyZurich, SwitzerlandVienna, AustriaFrankfurt, GermanyDusseldorf, GermanyAmsterdam, NetherlandsBrussels, BelgiumParis, FranceLondon, United KingdomManchester, United KingdomCopenhagen, DenmarkOslo, NorwayStockholm, SwedenHelsinki, FinlandWarsaw, PolandLagos, NigeriaJohannesburg, South AfricaCapretown, South AfricaTel Aviv, IsraelSaudi Arabia, Saudi ArabiaDubai, United Arab Emirates
		<div>ACAP (Asia-Pacific)</div> <ul style="list-style-type: none">New Delhi, IndiaMumbai, IndiaHyderabad, IndiaChennai, IndiaKuala Lumpur, MalaysiaSingapore, SingaporeHong Kong, ChinaTaipei, TaiwanShanghai, ChinaBeijing, ChinaTianjin, ChinaSeoul, South Korea



Part 2d. In-Scope Locations/Facilities

		<ul style="list-style-type: none">▪ Osaka, Japan▪ Tokyo, Japan▪ Perth, Australia▪ Melbourne, Australia▪ Canberra, Australia▪ Sydney, Australia▪ Auckland, New Zealand
--	--	---



Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions

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

☐ Yes ☒ No

Provide the following information regarding each item the entity 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)
Not applicable.	Not applicable.	Not applicable.	Not applicable.	Not applicable.

♦ 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, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.



Part 2. Executive Summary (continued)

Part 2f. Third-Party Service Providers

For the services being validated, does the entity have relationships with one or more third-party service providers that:

<ul style="list-style-type: none">Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<ul style="list-style-type: none">Manage system components included in the scope of the entity'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.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none">Could impact the security of the entity's CDE—for example, vendors providing support via remote access, and/or bespoke software developers.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

If Yes:

Name of service provider:	Description of service(s) provided:
Amazon Web Services (AWS)	Cloud hosting provider
Microsoft Azure	Cloud hosting provider

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



Part 2. Executive Summary (continued)

Part 2g. Summary of Assessment
(SAQ Section 2 and related appendices)

Indicate below all responses provided within each principal PCI DSS requirement.
For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

Note: One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed: Zscaler Cloud Service

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 Tested	Not in Place
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach



<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>1.2.6: There were no insecure services, protocols, or ports in use.</p> <p>1.4.4, 3.1.1 – 4.2.2, 7.2.6, 9.4.1 – 9.4.7, 12.7.10, A1.1.2: Zscaler did not store, process, or transmit CHD.</p> <p>1.3.3, 2.3.1, 2.3.2, 11.2.2: There were no wireless networks within or connected to the in-scope environment.</p> <p>5.2.3, 5.2.3.1: Antivirus was implemented on all system components capable of installing such software.</p> <p>5.3.2.1: Periodic malware scans were not performed to meet Requirement 5.3.2. Zscaler conducted continuous scans to meet Requirement 5.3.2.</p> <p>6.4.1: This requirement has been superseded by Requirement 6.4.2 as of March 31, 2025.</p> <p>6.4.3, 11.6.1: Zscaler did not maintain any payment pages.</p> <p>6.5.5: Zscaler did not utilize live PANs in pre-production or live production environments.</p> <p>8.2.3: No remote access to customer premises was available to users.</p> <p>8.2.7: Accounts assigned to third parties were not present in the user listings.</p> <p>8.3.6, 8.3.9: Biometrics and FIDO 2 tokens were utilized for authentication.</p> <p>8.3.10: This requirement has been superseded by Requirement 8.3.10.1 as of March 31, 2025.</p> <p>8.3.10.1: Zscaler did not provide customer users access to cardholder data.</p> <p>8.6.1: Interactive logins were disabled on application and/or system accounts.</p> <p>9.5.1 – 9.5.1.3, A2.1.1 – A2.1.3: Zscaler did not utilize POI or POS devices.</p> <p>10.7.1: This requirement has been superseded by Requirement 10.7.2 as of March 31, 2025.</p> <p>11.3.1.3, 11.3.2.1: No significant changes occurred to the in-scope environment during the previous 12 months.</p> <p>12.3.2: The customized approach was not utilized to fulfill any requirements in this assessment.</p> <p>12.5.3: No significant change to Zscaler's organization structure occurred during the previous 12 months.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not applicable.</p>



Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	August 19, 2025
Were any requirements in the SAQ unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated August 19, 2025.

Indicate below whether a full or partial PCI DSS assessment was completed:

- ☒ **Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.
- ☐ **Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

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

Select one:

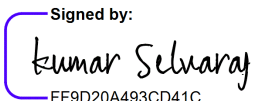
<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall COMPLIANT rating; thereby (Zscaler, Inc.) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>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 (Zscaler, Inc.) has not demonstrated compliance with the PCI DSS requirements included in this SAQ.</p> <p>Target Date for Compliance: <i>Not Applicable</i></p> <p>An entity 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></p>								
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more assessed 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 assessed 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 (Zscaler, Inc.) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted. <i>If selected, complete the following:</i></p> <table><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. Service Provider Acknowledgement****Signatory(s) confirms:****(Select all that apply)**

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, Version 4.0.1 was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Signed by:


FF9D20A493CD41C...

Signature of Service Provider Executive Officer ↑

Date: 11/5/2025

Service Provider Executive Officer Name: Kumar Selvaraj

Title: Vice President, Security and Compliance

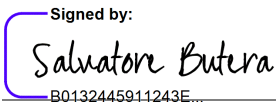
Part 3c. Qualified Security Assessor (QSA) Acknowledgement

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: QSA performed confirmation of control design and implementation along with review of this SAQ for completion.

Signed by:

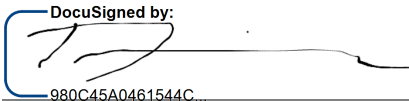

B0132445911243E...

Signature of Lead QSA ↑

Date: 11/5/2025

Lead QSA Name: Salvatore Butera

DocuSigned by:


980C45A0461544C...

Signature of Duly Authorized Officer of QSA Company ↑

Date: 11/5/2025

Duly Authorized Officer Name: Doug Barbin

QSA Company: Schellman Compliance, LLC

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: Not applicable



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 entity 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	
1	Install and maintain network security controls	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
3	Protect stored account data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
7	Restrict access to system components and cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
8	Identify users and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
10	Log and monitor all access to system components and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
11	Test security systems and networks regularly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for details of requirement applicability.

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/.