



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023



PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Equinix, Inc

Assessment End Date: November 1, 2024

Date of Report as noted in the Report on Compliance: November 15, 2024



Section 1: Assessment Information

Instructions for Submission

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

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	Equinix, Inc
DBA (doing business as):	Equinix
Company mailing address:	11 Devonshire Square, London, EC2M 4YR
Company main website:	www.equinix.com
Company contact name:	Hitesh Jivani
Company contact title:	Senior Manager, Global Operations Compliance
Contact phone number:	+44.(0)207.531.8629
Contact e-mail address:	Hitesh.Jivani@eu.equinix.com

Part 1b. Assessor (ROC Section 1.1)

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:	Mark Hatfield
Assessor phone number:	866.254.0000 ext. 927
Assessor e-mail address:	mark.hatfield@schellman.com
Assessor certificate number:	QSA, Credential ID: 206-674



Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed: Colocation Data Center Housing Services

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):

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POI / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

☐ 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):

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 Assessment (select all that apply):

Name of service(s) not assessed: All other services offered by Equinix

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):

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POI / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

☐ 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):

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

Only the physical security (data center/colocation) services offered by Equinix were included within the scope of this assessment. All services that fall under Interconnection, Connectivity, Network or Managed Services were not included within the scope of this assessment

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

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

Equinix does not store, process, or transmit cardholder data. Customers are responsible for all access to systems and data. Equinix provides secure space, power, and environmental controls for merchants and service providers, some of which are PCI compliant.



	Equinix has no logical access to any customer systems that may contain cardholder data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Equinix customers are responsible for all access to systems and data. Equinix has no logical access to any customer system that may contain cardholder data, and its managed and network Services are not within the scope of this assessment.
Describe system components that could impact the security of account data.	Equinix provides secure physical infrastructure (access controls, surveillance, environmental systems); customers are responsible for securing and maintaining system components to protect account data in compliance with PCI DSS requirements.

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.*

Equinix provides colocation services to merchants and service providers, some of which may store, process, or transmit cardholder data and fall under PCI compliance. Equinix does not store, process, or transmit cardholder data.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)

☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Colocation	255	AMER • Brazil: RJ1, RJ2, SP1, SP2, SP3, SP4, SP5x, • Canada: CL1, CL2, CL3, KA1, MT1, MT2, OT1, SJ1, TR1, TR2, TR5, TR6, TR7, VA1, WI1



		<ul style="list-style-type: none"> • Chile: ST1, ST2, ST3, ST4 • Colombia: BG1, BG2 • Mexico: MO1, MX1, MX2 • Peru: LM1 • Atlanta: AT1, AT4 • Boston: BO2 • Chicago: CH1, CH2, CH3, CH4, CH7 • Culpeper: CU1, CU2, CU3, CU4 • Dallas: DA1, DA2, DA3, DA4, DA6, DA7, DA9, DA11 • Denver: DE1, DE2 • Washington, DC: DC1, DC2, DC3, DC4, DC5, DC6, DC7, DC10, DC11, DC12, DC13, DC14, DC15, DC16, DC21, DC97 • Houston: HO1 • Los Angeles: LA1, LA2, LA3, LA4, LA7 • Miami: MI1, MI2, MI3, MI6 • New York: NY1, NY2, NY4, NY5, NY6, NY7, NY9, NY11, NY13 • Philadelphia: PH1 • Seattle: SE2, SE3, SE4 • Silicon Valley: SV1, SV2, SV3, SV4, SV5, SV8, SV10, SV11, SV12x, SV14, SV15, SV16 <p>APAC</p> <ul style="list-style-type: none"> • Australia: SY1, SY2, SY3, SY4, SY5, SY6, SY7, SY9x, ME1, ME2, ME4, ME5, AE1, BR1, CA1, PE1, PE2, PE3 • China: HK1, HK2, HK3, HK4, HK5, SH2, SH3, SH5, SH6 • India: MB1, MB2, MB4 • Japan: TY1, TY2, TY3, TY4, TY5, TY6, TY7, TY8, TY9, TY10, TY11, TY12x, TY13x, OS1, OS2x, OS3, OS4x • Malaysia: JH1, KL1 • South Korea: SL1, SL2x, SL4 • Singapore: SG1, SG2, SG3, SG4, SG5 <p>EMEA</p> <ul style="list-style-type: none"> • Bulgaria: SO1, SO2 • Finland: HE3, HE4, HE5, HE6, HE7 • France: BX1, PA2, PA3, PA4, PA5, PA6, PA7, PA8x, PA9x, PA10, PA13x • Germany: DU1, FR2, FR4, FR5, FR6, FR7, FR8, FR9x, FR11x, FR13, MU1, MU3, MU4, HH1 • Ireland: DB1, DB2, DB3, DB4, DB5x, DB6x • Italy: GN1, ML2, ML3, ML5, ML7x • Netherlands: AM1, AM2, AM3, AM4, AM5, AM6, AM7, AM8, AM11, EN1, ZW1 • Oman: MC1 • Poland: WA1, WA2, WA3, WA4x • Portugal: LS1
--	--	---



		<ul style="list-style-type: none">• Spain: MD1, MD2, MD3x, MD6, BA1• Sweden: SK1, SK2, SK3• Switzerland: GV1, GV2, ZH2, ZH4, ZH5• Turkey: IL2• UAE: DX1, DX2, DX3, AD1• United Kingdom: LD3, LD4, LD5, LD6, LD7, LD8, LD9, LD10, LD13x, LD11x, MA1, MA3, MA4, MA5
--	--	--

Part 2. Executive Summary (continued)

Part 2e. PCI SSC Validated Products and Solutions
(ROC Section 3.3)

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
Not applicable.	Not applicable.	Not applicable.	Not applicable.	Not applicable.

Part 2f. Third-Party Service Providers
(ROC Section 4.4)

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 entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	<input type="checkbox"/> Yes <input checked="" 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

* 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.



If Yes:	
Name of Service Provider:	Description of Services Provided:
Not applicable.	Not applicable.
Note: Requirement 12.8 applies to all entities in this list.	



Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

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: Colocation Data Center Housing Services

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach



For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

- 1.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.1.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.2.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.2.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.2.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.2.4 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.2.5 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.2.6 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.2.7 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.2.8 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.3.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.3.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.3.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.4.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.4.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.4.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.4.4 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.4.5 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 1.5.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 2.3.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 3.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 3.1.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 3.2.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 3.3.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.
- 3.3.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.3.1.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.3.1.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.3.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.3.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.4.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.4.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.5.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.5.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.5.1.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.5.1.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.6.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.6.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.6.1.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.6.1.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.6.1.4 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.4 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.5 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.6 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.7 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.8 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

3.7.9 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

4.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

4.1.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

4.2.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

4.2.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

4.2.1.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

4.2.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.2.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.2.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.2.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.2.3.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.2.4 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.3.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.4.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.4.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.4.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.5.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.5.4 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.5.5 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

6.5.6 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

7.2.6 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

8.2.3 - Not applicable. Interviews with Equinix personnel confirmed that Equinix did not have remote access to customer premises.

8.3.10 - Not applicable. Interviews with Equinix personnel confirmed that Equinix did not provide customer users with access to cardholder data.

8.3.10.1 - Not applicable. Interviews with Equinix personnel confirmed that Equinix did not provide customer users with access to cardholder data.

9.2.4 - Not Applicable. Equinix provided only physical security for customer systems. Colocation customers were responsible for ensuring their systems were kept in a "locked" state when not in use.

9.4.1 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement.

9.4.1.1 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement.

9.4.1.2 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement

9.4.2 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement

9.4.3 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement

9.4.4 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement

9.4.5 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement

9.4.5.1 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement

9.4.6 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement

9.4.7 - Not Applicable. Equinix did not maintain media containing cardholder data. Equinix customers were responsible for complying with this requirement

9.5.1 - Not Applicable. Equinix did not maintain any POS devices. Equinix customers were responsible for complying with this requirement.

9.5.1.1 - Not Applicable. Equinix did not maintain any POS devices. Equinix customers were responsible for complying with this requirement.

9.5.1.2 - Not Applicable. Equinix did not maintain any POS devices. Equinix customers were responsible for complying with this requirement.

9.5.1.2.1 - Not Applicable. Equinix did not maintain any POS devices. Equinix customers were responsible for complying with this requirement.

9.5.1.3 - Not Applicable. Equinix did not maintain any POS devices. Equinix customers were responsible for complying with this requirement.

10.2.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.2.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.2.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.3.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.3.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.3.1.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.3.1.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.3.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.3.2.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.4.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.4.2 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.4.3 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.4.4 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.4.5 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.4.6 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.4.7 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.5.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.5.1.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

11.6.1 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

12.3.2 - Not applicable. The customized approach was not utilized to fulfill any requirements in this assessment.

12.5.3 - Not applicable. This requirement is a best practice until March 31, 2025.

12.8.1 - Not Applicable. Equinix did not utilize service providers in relation to the assessed service.

12.8.2 - Not Applicable. Equinix did not utilize service providers in relation to the assessed service.

12.8.3 - Not Applicable. Equinix did not utilize service providers in relation to the assessed service.

12.8.4 - Not Applicable. Equinix did not utilize service providers in relation to the assessed service.

12.8.5 - Not Applicable. Equinix did not utilize service providers in relation to the assessed service.

12.10.7 - Not Applicable. Based on the scope of services, Equinix customers were responsible for complying with this requirement.

A1.1.1 - Not applicable. Equinix was not a multi-tenant service provider.

A1.1.2 - Not applicable. Equinix was not a multi-tenant service provider.

A1.1.3 - Not applicable. Equinix was not a multi-tenant service provider.

A1.1.4 - Not applicable. Equinix was not a multi-tenant service provider.

A1.2.1 - Not applicable. Equinix was not a multi-tenant service provider.

A1.2.2 - Not applicable. Equinix was not a multi-tenant service provider.

A1.2.3 - Not applicable. Equinix was not a multi-tenant service provider.

A2.1.1 - Not applicable. Equinix did not use SSL/Early TLS or POI terminals

A2.1.2 - Not applicable. Equinix did not use SSL/Early TLS or POI terminals

A2.1.3 - Not applicable. Equinix did not use SSL/Early TLS or POI terminals

For any Not Tested responses, identify which sub-requirements were not tested and the reason.

2.1.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.1.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.2.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.2.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.2.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.2.4 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.2.5 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.2.6 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.2.7 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

2.3.1 - Based on the scope of services, Equinix customers were responsible for complying with this requirement.

5.1.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.1.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.2.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.2.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.2.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.2.3.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.3.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.3.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.3.2.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.3.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.3.4 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.3.5 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

5.4.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

6.1.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

6.1.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

6.3.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

6.3.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

6.5.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

6.5.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.1.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.1.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.2.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.2.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.2.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.2.4 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.2.5 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.2.5.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.3.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.3.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

7.3.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.1.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.1.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.2.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.2.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.2.4 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.2.5 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.2.6 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.2.7 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.2.8 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.4 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.5 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.6 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.7 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.8 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.9 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.3.11 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.4.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.4.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.4.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.5.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.6.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.6.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

8.6.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.1.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.1.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.2.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.2.1.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.2.1.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.2.1.4 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.2.1.5 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.2.1.6 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.2.1.7 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.2.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.3.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.3.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.3.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.3.4 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.4.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.4.1.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.4.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.4.2.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.4.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.5.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.6.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.6.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

10.6.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

11.1.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

11.1.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

11.5.2 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

12.2.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

12.3.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

12.3.3 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

12.3.4 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.

12.5.1 - The logical access and configuration management controls of the physical access systems were not tested. For all other system-level controls, Equinix customers were responsible for complying with this requirement.



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>		September 16, 2024
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>		November 1, 2024
Were any requirements in the ROC unable to be met due to a legal constraint?		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Examine documentation	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
• Interview personnel	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
• Examine/observe live data	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
• Observe process being performed	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
• Observe physical environment	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
• Interactive testing	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
• Other: Not Applicable	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	



Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated November 15, 2024.

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

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

Based on the results documented in the ROC 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 ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT rating; thereby <i>Equinix, Inc</i> has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating; thereby <i>Equinix, Inc</i> has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance: Not Applicable.</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 before completing Part 4.</p>								
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more assessed requirements in the ROC 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 In Place or Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby <i>Equinix, Inc</i> has demonstrated compliance with all PCI DSS requirements 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.</p> <p><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 3. PCI DSS Validation *(continued)*

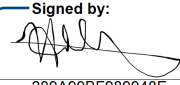
Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

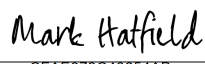
<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the 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.

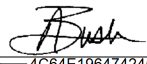
Part 3b. Service Provider Attestation

Signed by: 	
289A99BF989948E... Signature of Service Provider Executive Officer ↑	Date: 11/15/2024
Service Provider Executive Officer Name: Hitesh Jivani	Title: Senior Manager, Global Operations Compliance

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance.
If selected, describe all role(s) performed: Independent Assessor	

Signed by: 	
CFAE073C40654AB... Signature of Lead QSA ↑	Date: 11/15/2024
Lead QSA Name: Mark Hatfield	

DocuSigned by: 	
4C64E1964742453... Signature of Duly Authorized Officer of QSA Company ↑	Date: 11/15/2024
Duly Authorized Officer Name: Adam Bush	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:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> 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 Non-Compliant results 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 provide 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 requirement applicability.
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
3	Protect stored account data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for 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 requirement applicability.
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for 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 requirement applicability.
8	Identify users and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for 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 requirement applicability.
11	Test security systems and networks regularly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for 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 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 requirement applicability.

