



# 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**

Revision 2

Publication Date: August 2023

## 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:	RazorPay Technologies Private Limited
DBA (doing business as):	
Company mailing address:	SJR Cyber, Hosur Rd, Konappana Agrahara, Adugodi, Bengaluru, Karnataka
Company main website:	<a href="https://razorpay.com/">https://razorpay.com/</a>
Company contact name:	Hilal Lone
Company contact title:	Senior Director, Information Security and Compliance (CISO)
Contact phone number:	+91 7006717459
Contact e-mail address:	hilal.lone@razorpay.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):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

## 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:		
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input checked="" type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> 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 PCI DSS Assessment** (select all that apply):

Name of service(s) not assessed:	Not Applicable
Type of service(s) not assessed:	

<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:		

<b>Part 2b. Description of Role with Payment Cards</b>	
Describe how the business stores, processes, and/or transmits account data.	<p>Razorpay Technologies Private Limited (RTPL) is a company with a vision to become a prominent provider of full-stack issuing platforms for store-of-value products like Gift Cards and Wallets. Their mission is to equip consumer-facing businesses with innovative solutions that not only optimize costs but also enhance customer retention and boost spending.</p> <p>RTPL 'Wallet as a Service' aims to offer merchants with another Wallet as a Service product, a co-branded prepaid wallet with RBI-complaint functionality and the ability to expand acceptance of this payment method outside their own ecosystem.</p> <p>With this product, the merchants will be able to</p> <ol style="list-style-type: none"> <li>1. Offer an off-the-shelf 'plug-n-play' wallet to their customers</li> <li>2. Enable a single-click checkout experience to their customers holding wallet</li> </ol>

	<ol style="list-style-type: none"> <li>3. Reduce dependency on third-party authentication across various payment methods</li> <li>4. Allow users to split their transaction amount across wallet and other payment modes</li> <li>5. Enable instant refunds to users for failed/canceled orders</li> <li>6. Enables merchants to run campaigns and promotions by providing cashback and other offers</li> <li>7. Enables merchants to provide wallet linked services to consumers such as wallet balance inquiry and transaction history, recurring payments via linked wallet etc.</li> </ol> <p>Merchants will also get access to an admin dashboard to track wallet usage patterns, collect refunds for canceled/failed orders and lure Wallet users with offers, cashback etc. to revive them on their own platform.</p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not Applicable
Describe system components that could impact the security of account data.	Not Applicable

**Part 2. Executive Summary** *(continued)*

**Part 2c. Description of Payment Card Environment**

<p>Provide a <b>high-level</b> description of the environment covered by this assessment.</p> <p><i>For example:</i></p> <ul style="list-style-type: none"> <li>• <i>Connections into and out of the cardholder data environment (CDE).</i></li> <li>• <i>Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i></li> <li>• <i>System components that could impact the security of account data.</i></li> </ul>	<p>Razorpay Technologies Private Limited (RTPL) is a wallet solution company in India that allows businesses to issue wallets to customers, load cashbacks or promotions to their wallets and accept payments from those wallets. This helps merchants provide discounts/cashbacks and increase customer loyalty.</p> <p>RTPL's infrastructure consists of workstations, domain controllers, firewalls, and internet connectivity used to connect to the Razorpay network. RTPL manages the operating system for servers, network, and security devices and software such as anti-virus, network scanners, and log management applications. All core applications are hosted within the datacenter located in Amazon Web Services (AWS). RTPL provides its services to user entities using the infrastructure hosted on Amazon Web Services (AWS), a third-party cloud service provider.</p>
<p>Indicate whether the environment includes segmentation to reduce the scope of the assessment.</p> <p><i>(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)</i></p>	<p><input type="checkbox"/> Yes   <input checked="" type="checkbox"/> No</p>

**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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
AWS Data Center	1	Mumbai, India

**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<sup>1\*</sup>?

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)

<sup>1</sup> 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](http://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"> <li>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)</li> </ul>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<ul style="list-style-type: none"> <li>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.</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>Could impact the security of the entity's CDE↓for example, vendors providing support via remote access, and/or bespoke software developers.</li> </ul>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

**If Yes:**

Name of service provider:	Description of service(s) provided:
Amazon Web Services, Inc	Cloud hosting provider
Razorpay Software Pvt Ltd	Payment & API Gateway
RazorpayX Private Limited	Payouts/Bank Transfers to wallet holders

**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:** Wallet Services

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 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**

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

1.2.6 is Not Applicable as these is no services protocols and ports are in use which is considered to be insecure.

1.3.3 is Not Applicable as wireless network is not present in scoped environment

2.2.5 is Not Applicable as entity doesn't utilize any insecure services across the scoped environment.

2.3.1 is Not Applicable as wireless network is not present in scoped environment to access cardholder data.

2.3.2, 3.3.2, Is Not Applicable as wireless network is not present in scoped environment to access cardholder data.

3.2.1, 3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3, 4.2.1,4.2.1.1, 4.2.1.2, 4.2.2, 3.3.3, 3.4.1, 3.4.2, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3 Is not applicable as entity do not store, transmit ro process cardholder data.

3.6.1,3.6.1.1, 3.6.1.2, 3.6.1.3, 3.6.1.4, 3.7.1,3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.6, 3.7.7, 3.7.8, 3.7.9 not Applicable as entity do not store and share any cryptographic key with customer.

4.2.1.2 is Not Applicable as entity doesn't utilize wireless networks for transmitting cardholder data across RTPL scoped environment.

5.2.1 is Not Applicable as there are no systems present in the scoped environment which can be commonly affected by malware

5.2.3 Is Not Applicable as there are no systems considered to be not commonly affected by malicious software.

5.3.3 Is Not Applicable as there is no removable media allowed.

5.4 Is Not Applicable As this requirement is best practice

6.3.2, 6.4.2, 6.4.3, 7.2.4, 7.2.5, 7.2.5.1, 8.3.10, 8.3.10.1, 8.4.2, 8.5.1, 8.6.1 8.6.2, 8.6.3 Is Not Applicable As this requirement is best practice

8.2.7 Is Not Applicable as there are no third parties having access to scoped environment.

9.2.3, are Is Not Applicable as the assessed entity does not take physical media backup of cardholder data

9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3 , 9.4.4 , 9.4.5 9.4.5.1 9.4.6 , 9.4.7 , Is Not Applicable as there are no physical media storing cardholder data.

9.5.1.2, 9.5.1.1, 9.5.1.3, is Is Not Applicable as the assessed entity does not involve transaction and/or maintenance of POI devices

9.5.1.2.1 Is Not Applicable As this requirement is best practice

10.4.1.1, 10.4.2.1, 10.7.2, 11.3.1.1, 11.3.1.2, 11.4.7 Is Not Applicable As this requirement is best practice

11.5.1.1 is Not Applicable As this requirement is best practice

11.6.1, 12.3.1 is Not Applicable As this requirement is best practice

	<p>11.2.2 not Applicable as there is no wireless access points in the scoped environment.</p> <p>12.3.3, 12.3.4, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.1, 12.6.3.2, 12.10.4.1, 12.10.5, 12.10.7 Is Not Applicable As this requirement is best practice</p> <p>Entire Appendix A1 is Is Not Applicable as assessed entity is not a shared hosting service provider. Entire Appendix A2 is Is Not Applicable as SSL and/or early TLS are not used for POS/POI terminals in the scoped environment.</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:	2023-10-06
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 (Self-assessment completion date 2023-10-06).

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><b>Compliant:</b> 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 <b>COMPLIANT</b> rating; thereby (<i>Razorpay Technologies Private Limited</i>) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p><b>Non-Compliant:</b> 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 <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated compliance with the PCI DSS requirements included in this SAQ.</p> <p><b>Target Date</b> for Compliance: YYYY-MM-DD</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><b>Compliant but with Legal exception:</b> 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 <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby (<i>Service Provider Company Name</i>) 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 border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 40%;">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 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

*Hilal Lone*

Authenticated through  
Leegality.com (qLMDaeY)  
Hilal Lone  
Date: Wed Oct 25 14:58:19 IST  
2023

Signature of Service Provider Executive Officer <input type="checkbox"/>	Date: 2023-10-17
Service Provider Executive Officer Name: Hilal Lone	Title: Senior Director, Information 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:

Signature of Lead QSA <input type="checkbox"/>	Date: YYYY-MM-DD
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company <input type="checkbox"/>	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 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"/>	
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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"/>	

