



# 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: Tripode Partners Group S.L.**

**Assessment End Date: 27 September 2024**

**Date of Report as noted in the Report on Compliance: 27 September 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:	Tripode Partners Group S.L.
DBA (doing business as):	Dingus Spain S.L
Company mailing address:	C/ Galileo Galilei 2, Edf U, Local 01, 07121 Parc Bit, Illes Balears, Spain
Company main website:	<a href="https://www.dingus.es/">https://www.dingus.es/</a>
Company contact name:	Óscar Sánchez
Company contact title:	Responsable seguridad
Contact phone number:	+34 682 609 244
Contact e-mail address:	<a href="mailto:oscar.sanchez@dingus.es">oscar.sanchez@dingus.es</a>

##### 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):	N/A
Qualified Security Assessor	
Company name:	A2 Secure Tecnologias Informatica, Sociedad Ltd.
Company mailing address:	Av. de Francesc Cambó, 21, 10a. 08003 Barcelona (Spain)
Company website:	<a href="https://www.a2secure.com/">https://www.a2secure.com/</a>
Lead Assessor name:	Guillem Cuesta
Assessor phone number:	933 94 56 00
Assessor e-mail address:	<a href="mailto:guillem.cuesta@a2secure.com">guillem.cuesta@a2secure.com</a>
Assessor certificate number:	205-308

## 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:		Book&Payment
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 checked="" 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 checked="" type="checkbox"/> Others (specify): CRS-Central Reservation System		

**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 Tripode Partners Group S.L. services not specifically listed above

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:

-

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

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

Dingus is a company with software products such as hotel distribution software, which helps hotels manage and distribute their bookings across multiple online channels. Its goal is to simplify reservation management, optimize occupancy, and maximize revenue by integrating booking systems, distribution channels, and other related services.

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

Book&Payment environments does not store CHD. However, some data (PAN and CVV) is received and processed by the solution.

Describe system components that could impact the security of account data.

Dingus manages the PCI environment deployed on AWS, which includes both public and private subnets. The following services and functions impact the security of account data:

**Public Subnet:**

- Elastic Load Balancer (ELB): The ELB is responsible for distributing incoming traffic across multiple instances, which helps in balancing the load and preventing any single point of failure. Its configuration and security settings are critical for ensuring secure and reliable access to the environment.
- Bastion Host: The Bastion host provides sysadmin access through SSH to manage and monitor the instances in the private subnet. Its security is essential to prevent unauthorized access and ensure that sysadmin operations are conducted securely.

**Private Subnet:**

- API Servers: These servers handle application processing and communication within the private network. Their security is crucial as they interact with sensitive data and contribute to the overall protection of account data.
- Main Database (MongoDB): The MongoDB instance stores data, including any tokens or transaction information. Proper configuration, access controls, and encryption of the database are essential to protect stored data.
- Wazuh: This security monitoring service provides intrusion detection and log analysis, which helps in identifying and responding to potential security threats. Effective use of Wazuh is key to maintaining the security of account data by detecting and mitigating risks.

**Access Controls:**

- Two-Factor Authentication (2FA): Access to the environment is secured through 2FA, which adds an additional layer of security by requiring two forms of verification before access is granted. This helps in preventing unauthorized access to the PCI environment and ensures that only authorized personnel can access sensitive components.

Overall, the managed services and functions provided by the organization are designed to enhance the security of account data by implementing robust access controls,

---

	balancing loads, securing database interactions, and monitoring for potential threats.
--	--

---

## 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.*

All PCI environment has been deployed on AWS (Amazon Web Services) by Dingus.

The PCI environment includes 2 VPC (Public Subnet & Private Subnet) where all required instances are allocated.

While on the public subnet Dingus has allocated the ELB and the BASTION (sysadmin access through SSH), the API servers, the main DB (Mongo DB), Wazuh and other management services has been deployed on the private network.

The access to the environment is performed through a 2FA.

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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Dingus headquarters	1	Palma Mallorca, Spain
AWS environment	1	eu-west-1 Europe (Ireland)



## 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
N/A	N/A	N/A	N/A	N/A

---

\* 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 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"> <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 checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• 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)</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 checked="" type="checkbox"/> Yes <input type="checkbox"/> No

**If Yes:**

<b>Name of Service Provider:</b>	<b>Description of Services Provided:</b>
Amazon WebServices (AWS)	On-demand cloud computing platform
Addon Payments	Payment processing
PAYCOMMET	Payment processing
PayNoPain	Payment processing
Redsys	Payment processing
UniversalPay	Payment processing
Banca March through Redsys	Payment processing
Abreu Online	OTA (Online travel Agency)
Agoda	OTA (Online travel Agency)
ATRAPALO	OTA (Online travel Agency)
BOOKING	Travel fare aggregator
CHECK24	OTA (Online travel Agency)
CTRIP	OTA (Online travel Agency)
DESPEGAR	OTA (Online travel Agency)
EDREAMS	OTA (Online travel Agency)
EXPEDIA	Travel fare aggregator
FASTPAY	OTA (Online travel Agency)
GNA Hotel Solutions	OTA (Online travel Agency)
HBSI	OTA (Online travel Agency)
HOTELBEDS	OTA (Online travel Agency)

Hotetec	OTA (Online travel Agency)
Hotusa	OTA (Online travel Agency)
IGM WEB	OTA (Online travel Agency)
Lastminute	OTA (Online travel Agency)
LIBGO TRAVEL/FLIGHT CENTRE	OTA (Online travel Agency)
Mirai	OTA (Online travel Agency)
Neobookings	OTA (Online travel Agency)
PARATY	OTA (Online travel Agency)
ROIBACK	OTA (Online travel Agency)
SEE USA TOURS	OTA (Online travel Agency)
TRAFFICS/CONNECTED DESTINATIONS	OTA (Online travel Agency)
TRAVELREPUBLIC/DNATA	OTA (Online travel Agency)
W2M/NT INCOMING	OTA (Online travel Agency)
Welcomebeds	OTA (Online travel Agency)

**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: Book&Payment

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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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

<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p><b>1.2.6, 2.2.5.b</b> It was verified that the organization does not allow the usage of insecure services, daemons, or protocols in the CDE.</p> <p><b>1.3.3</b> It was verified that the organization does not transmit cardholder data over wireless networks, nor does it use these networks in any way that could impact the security of the CDE</p> <p><b>1.4.4, 3.4.1 through 3.7.9</b> The organization does not store cardholder data</p> <p><b>2.3.1</b> The organization does not transmit cardholder data over wireless networks, nor does it use these networks in any way that could impact the security of the CDE</p> <p><b>3.3.3</b> The organization does not support issuing services</p> <p><b>4.2.1</b> Considered Security Best practice until 31 March 2025</p> <p><b>4.2.2</b> PANs are not allowed to be sent through end-user messaging technologies.</p> <p><b>5.2.3.1, 5.3.2.1</b> Considered Security Best practice until 31 March 2025</p> <p><b>6.3.2, 6.4.3</b> Considered Security Best practice until 31 March 2025</p> <p><b>7.2.4.b, 7.2.5.b, 7.2.5.1, 7.2.6.b</b> Considered Security Best practice until 31 March 2025</p> <p><b>8.2.4</b> There have been no new additions</p> <p><b>8.2.5.a</b> There have been no terminations</p> <p><b>8.2.5.b, 8.3.11</b> The organization does not use physical authentication factors</p> <p><b>8.3.10.1, 8.5.1, 8.6.1, 8.6.2.b, 8.6.3</b> Considered Security Best practice until 31 March 2025</p> <p><b>9.4.1 through 9.5.1</b> The organization's PCI environment does not include external storage media such as backups or tapes that can be transported, classified, etc. All scope is located in AWS.</p> <p><b>10.7.2, 10.7.3, 11.3.1.1, 11.3.1.2, 11.4.7, 11.5.1.1, 11.6.1, 12.3.1, 12.3.3, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3, 12.10.4.1, 12.10.7</b> Considered Security Best practice until 31 March 2025</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	

## 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>		25 July 2024
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>		27 September 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 checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Other: -	<input type="checkbox"/> Yes	<input 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 *(Date of Report as noted in the ROC 27 September 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)*:

**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 *Tripode Partners Group S.L.* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

**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 *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.

**Target Date** for Compliance: YYYY-MM-DD

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.

**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 *(Service Provider Company Name)* 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.

This option requires additional review from the entity to which this AOC will be submitted.

*If selected, complete the following:*

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

### 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

Signature of Service Provider Executive Officer 	Date: <b>27 September 2024</b>
Service Provider Executive Officer Name: <b>Óscar Sánchez</b>	Title: <b>Responsable seguridad</b>

#### 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 checked="" type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed: QSA has assisted with PCI-DSS insights and advice on how to interpret the requirements but has not conducted a formal PCI DSS audit.

  <small>CIF: B-65040107</small>	<small>Avda. Francesc Cambó 21, 10<sup>a</sup>          08003 Barcelona          T: 93 394 56 00          F: 93 394 56 01</small>
Signature of Lead QSA 	Date: <b>27 September 2024</b>
Lead QSA Name: <b>Guillem Cuesta</b>	

  <small>CIF: B-65040107</small>	<small>Avda. Francesc Cambó 21, 10<sup>a</sup>          08003 Barcelona          T: 93 394 56 00          F: 93 394 56 01</small>
Signature of Duly Authorized Officer of QSA Company 	Date: <b>27 September 2024</b>
Duly Authorized Officer Name: <b>Albert Morell</b>	QSA Company: <b>A2 Secure Tecnologias</b>



Informatica S.L.

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

