

# CERTIFICATE OF COMPLIANCE WITH PCI DSS

AWARDED TO

Quipu GmbH



**ASSESSED BY INTEGRITY360 EUROPE LIMITED AND FOUND TO BE COMPLIANT  
WITH PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD V4.0.1**



**WEBSITE** <http://www.quipu.de/>  
**CATEGORY** Service Provider  
**ASSESSMENT** Level 1

*Alessandro Amalfitano*  
**ALESSANDRO AMALFITANO**  
PAYMENTS COMPLIANCE PRACTICE MANAGER

**COMPLIANCE DATE** 27 March, 2025  
**EXPIRATION DATE** 26 March, 2026

INTEGRITY360 EUROPE LIMITED has issued this certificate to indicate that the aforementioned company has been assessed against the objectives of Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures and were found to be compliant with PCI DSS, on the date of issue only, no other guarantees given. This certificate is to be used in conjunction with the Attestation of Compliance (AOC) for a detailed description of the services included in the scope of the PCI DSS Assessment. This certificate offers no guarantee or warranty to any third party that the company is invulnerable to attack or breaches in its security, integrity or availability, and INTEGRITY360 EUROPE LIMITED accordingly accepts no liability to any third party in the event of loss or damage of any description caused by any failure in or breach of customer's security.

Certificate ID: OINuAPIGByXgiaQ

**INTEGRITY360.COM**



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0.1**

Publication Date: August 2024



## **PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: Quipu GmbH**

**Date of Report as noted in the Report on Compliance: 27 March 2025**

**Date Assessment Ended: 27 March 2025**

## 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:	Quipu GmbH
DBA (doing business as):	N/A
Company mailing address:	Königsberger Str. 1, 60487 Frankfurt/Main, Germany
Company main website:	<a href="http://www.quipu.de/">http://www.quipu.de/</a>
Company contact name:	[REDACTED]
Company contact title:	[REDACTED]
Contact phone number:	[REDACTED]
Contact e-mail address:	[REDACTED]

##### 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:	INTEGRITY360 EUROPE LIMITED
Company mailing address:	Termini, 3 Arkle Rd, Sandyford Business Park, Sandyford, Dublin 18, Ireland, D18 T6T7
Company website:	<a href="http://www.integrity360.com">www.integrity360.com</a>
Lead Assessor name:	[REDACTED]
Assessor phone number:	[REDACTED]
Assessor e-mail address:	[REDACTED]
Assessor certificate number:	[REDACTED]



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:		QPC acquiring, 3D Secure and e-commerce services	
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 checked="" 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 checked="" type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input checked="" type="checkbox"/> ATM <input checked="" type="checkbox"/> Other processing (specify): 3D Secure, E-commerce Acquiring	
<input checked="" type="checkbox"/> Account Management	<input checked="" type="checkbox"/> Fraud and Chargeback	<input checked="" 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 checked="" 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): Monitoring			

**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:		N/A
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:		N/A

Part 2b. Description of Role with Payment Cards  
(ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	<p>As a processing center, Quipu receives, stores, processes and transmits CHD and SAD as a part of authorization and clearing.</p> <p>Storage: data is in encrypted files (RSA-2048, clearing) and encrypted database (Oracle TDE, AES 256).</p> <p>Processing: All processing functionality is performed by TranzWare PCI SSF validated software suite. This software is currently undergoing Secure Software validation.</p> <p>Receiving and transmitting: through EFT (authorization) and secure file transfer (SFTP for clearing files).</p>
---	--



	All CHD and SAD exchange is performed electronically through encrypted (TLS 1.2 with strong ciphers) channels from POS, ATM or e-commerce to authorization platform.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	<p>As a processing center performing issuing and acquiring services, Quipu needs to have the ability to process, store and transmit CHD and SAD. Note that SAD is never stored on non-volatile storage and is only processed in RAM.</p> <p>The Kosovo-based Quipu Sh.P.K. Card Personalization Centre, involved in data preparation and card issuing business and serviced by QPC, is not part of the current assessment.</p>
Describe system components that could impact the security of account data.	N/A



Part 2. Executive Summary (continued)

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment.

For example:

- Connections into and out of the cardholder data environment (CDE).
- Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.
- System components that could impact the security of account data.

The CDE consists of Cisco firewalls, routers, switches, physical and virtual Windows servers and supporting software (IDS, FIM, AV).

QPC uses the PCI Software Standard certified payment application TranzWare Suite, developed by Compass Plus Ltd. Cardholder data is stored in a database encrypted with 256-bit AES and flat files encrypted with RSA 2048-bit encryption. The data transferred from and to the banks and card schemes over open public networks is secured with encrypted VPNs. The payment platform is operated by personnel located in Frankfurt/Main, Germany. The administrative communication from the office to the data center is secured by MFA.

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)
Example: Data centers	3	Boston, MA, USA
Corporate office	1	Frankfurt/Main, Germany
Data centers	2	Equinix FR2: Frankfurt/Main, Germany Equinix FR4: Frankfurt/Main, Germany





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
TranzWare Suite	3.2	Secure Software Standard v1.2.1	24-44.01489.002	2028-01-10
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

\* 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, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.



Part 2. Executive Summary (continued)

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:

• 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 checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• 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 checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Could impact the security of the entity’s CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Services Provided:
Compass Plus Ltd.	Software supplier.
Equinix	Data center & colocation provider.

**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: QPC acquiring, 3D Secure and e-commerce services

PCI DSS Requirement	Requirement Finding				Select If a Compensating Control(s) Was Used
	More than one response may be selected for a given requirement. Indicate all responses that apply.				
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" 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"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" 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"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" 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"/>
Requirement 7:	<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"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" 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"/>
Requirement 11:	<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 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"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" 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>1.2.6 - N/A, there were no services, protocols or ports that could be considered insecure.</p> <p>2.2.5 - N/A, no insecure services, protocols or daemons are present in the scope.</p> <p>2.3.1, 2.3.2, 4.2.1.2 - N/A, there were no wireless environments in or connected to the CDE.</p> <p>3.3.3 - N/A, Quipu does not provide or support any issuing services.</p> <p>3.5.1.1 - N/A, hashing was not utilized for rendering PAN unreadable.</p> <p>3.5.1.2, 3.5.1.3, - N/A, disk-level encryption was not utilized by Quipu to render PAN unreadable.</p> <p>3.7.2 - N/A, no cryptographic key distribution is performed.</p> <p>3.7.9 - N/A, Quipu does not share cryptographic keys with its customers.</p> <p>6.4.3, 10.4.1.1 - N/A, these requirements are best practice until 31 March 2025.</p> <p>4.2.2 - N/A, PAN is prohibited from being sent via end-user messaging technologies under any circumstances.</p> <p>5.2.3, 5.2.3.1 - N/A, anti-malware is installed on all types of CDE components.</p> <p>6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.3.1 - N/A, no software applications are developed for use within the CDE that are in scope of this Report on Compliance.</p> <p>8.2.2 - N/A, no group, shared, or generic IDs are utilized.</p> <p>8.2.3 - N/A, Quipu does not have remote access to customer premises.</p> <p>8.2.7 - N/A, no third parties or vendors with remote access to the cardholder data environment.</p> <p>8.3.10, 8.3.10.1 - N/A, Quipu is a service provider but does not provide customer passwords.</p> <p>9.4.3, 9.4.4 - N/A, media is not sent out of the Quipu facilities.</p> <p>9.5.1-9.5.1.3, A2 - N/A, there are no devices that capture payment card data via direct physical interaction with the card within Quipu's CDE.</p> <p>11.4.7, A1 - N/A, Quipu is not a multi-tenant service provider.</p> <p>12.3.2 - N/A, During the course of the assessment the assessor did not identify any requirements met by Quipu with the Customized Approach.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not Applicable.</p>



## Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: <i><b>Note:</b> This is the first date that evidence was gathered, or observations were made.</i>	2025-02-07
Date Assessment ended: <i><b>Note:</b> This is the last date that evidence was gathered, or observations were made.</i>	2025-03-27
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?	<input checked="" 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 2025-03-27).*
- 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 Quipu GmbH 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)*

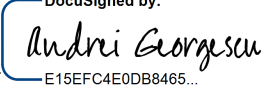
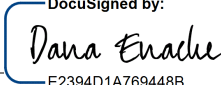
### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 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

DocuSigned by:  <small>E15EFC4E0DB8465...</small> Signature of Service Provider Executive Officer ↑	DocuSigned by:  <small>E2394D1A769448B...</small> Signature of Service Provider Executive Officer ↑	Date: 2025-03-27
Service Provider Executive Officer Name: Andrei Georgescu, Dana Enache		Title: Managing Director, Managing Director

### 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:
Signature of Lead QSA ↑	
Date: 2025-03-27	
Signature of Duly Authorized Officer of QSA Company ↑	
Date: 2025-03-27	
QSA Company: INTEGRITY360 EUROPE LIMITED	

### 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: N/A



## 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"/>	

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/)*