



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: Tecnes Milano s.r.l.

Date of Report as noted in the Report on Compliance: 2024-11-22

Date Assessment Ended: 2024-11-22

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:	Tecnes Milano s.r.l.
DBA (doing business as):	Room Cloud
Company mailing address:	Mailing address: Via Piranesi 26 – 20137 Milano (MI) - Italy
Company main website:	Company main website: http://www.tecnes.com
Company contact name:	Leopoldo Sergi
Company contact title:	CEO
Contact phone number:	+39.0267101036
Contact e-mail address:	l.sergi@tecnes.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):	n.a.
Qualified Security Assessor	
Company name:	RISC3 Srl
Company mailing address:	Via A. Volta, 3. 10121 Torino (TO) - Italy
Company website:	www.risc3.com
Lead Assessor name:	Giuseppe Citro
Assessor phone number:	+39 3383701481
Assessor e-mail address:	giuseppe.citro@risc3.com
Assessor certificate number:	205-054

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:		Channel Manager Hotel Booking Engine	
Type of service(s) assessed:			
Hosting Provider: <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):	Managed Services: <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):	Payment Processing: <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 checked="" 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):			
<p>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.</p>			

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: Web design, system integration

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): ICT consultancy

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

The services checked are non included in the assessment because they aren't related to CHD management

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.

Tecnes developed two tools for the accommodation market: a booking engine and a channel manager. The first is dedicated to the accommodation facilities that sell their services directly through their web sites; the second is dedicated to the accommodation facilities that sell their services through third party portals. Tecnes sells the tools 'as a service', so it's considered as a service provider.

Both the tools collect and store the reservation data received by the accommodation facilities, including the

	<p>CHD, if any. They manage about 450.000 reservations a month.</p> <p>The reservation data are stored for management Purposes, the CHDs are stored as a guarantee for the accommodation facilities in case of the customers leave the hotel w/o paying for the accommodation, cancel a nonrefundable reservation, or do not show up without notice on the day established for the start of the stay,</p> <p>The booking engine receives the reservations data from the accommodation's facility. The connection between the accommodation facilities' websites and the booking engine is secured.</p> <p>The channel manager connects to each channel and gets the reservation data. This connection is secured, too.</p> <p>Both the booking engine and the channel manager store the reservation data on the same repository, In the repository, the data are stored encrypted and removed at checkout after that accommodation facilities confirm this by reading the data. In any case, if the SAD is not read, at maximum the SAD is maintained until the checkout of the accommodation facilities' customers</p> <p>The accommodation facilities can see the reservation data passing a two-level authentication process: using the first level account they can see the reservation data without the CHD, and using the second level account they can see also the CHD. Is possible to read the CHD just two times:</p> <ol style="list-style-type: none"> 1. Card verification by the hotelier (with a display of the CAV2, CVC2, CID, or CVV2 , the first of the two allowed vision) 2. When the hotelier makes the payment transaction
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>Tecnes never uses the stored CHD to make payments. It has the ability to impact the security of the cardholder data because it receives, stores and transmits CHD, it develops the tools used to manage the CHD and it administers the infrastructure used for this purposes.</p>
<p>Describe system components that could impact the security of account data.</p>	<ul style="list-style-type: none"> - Firewall Systems: Protect the Cardholder Data Environment (CDE) by controlling and monitoring traffic between trusted and untrusted networks. - Web Application: Applications that interact with the CDE Ensures data transmission is encrypted (e.g., TLS 1.2 or higher). Authentication mechanisms to ensure only legitimate transactions are processed. - Input/Output CHD flow with partner: Process CHD and communicate with external partner - Database Servers:

Store CHD securely on behalf of customers.

- Encryption and Key Management Systems:
Securely manage the encryption keys used to protect CHD.
- Logging and Monitoring Systems:
Record and monitor activities within the CDE to identify and respond to security incidents.
- Administrative Systems:
Google console used by administrators to manage and maintain the CDE and its components..

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.*

Tecnes build his Infrastructure on the GCP (Google Cloud Platform). GCP includes a range of hosted services for compute, storage and application development that run on Google hardware. Google Cloud Platform services can be accessed by software developers, cloud administrators, and other enterprises IT professionals. Tecnes's employees connect to GCP over the public internet. The Tecnes's datacenter in GCP is a virtual infrastructure that maintains the functioning of the services, the main DB, and Software development and maintenance.

The CHD are received through the internet. (accommodation facility's web site or connecting to the channel repository) over secured connections . The CHD are transmitted over the Internet (web Interface or API) using secure connections

The CHD passes from the booking engine and the channel manager front ends (web based or API) In the repository (database) through API.

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>
Datacenter	1	c/o Google (Google Compute Engine) europe-west3-c Francoforte, Germania, Europa europe-west3-b Francoforte, Germania, Europa europe-west2-c Londra, Inghilterra, Europa europe-west1-b Saint-Ghislain, Belgio, Europa

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
				YYYY-MM-DD
				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) (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:

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

If Yes:

Name of Service Provider:	Description of Services Provided:
Google, LLC	Hosting Service Provider, it provides the Google Cloud Platform (GCP) technologies and infrastructure managed by Google

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: Channel Manager Hotel Booking Engine

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	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 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>1.3.3, 2.3.1, 2.3.2 N.A. Tecnes doesn't build wireless networks</p> <p>2.2.5 N.A. No insecure services, daemons, or protocols are enabled</p> <p>3.3.1.1 N.A. because Tecnes does not receive or process any full-track data</p> <p>3.3.1.3 N.A. because Tecnes does not receive or process PIN data</p> <p>3.3.3 N.A. because Tecnes is not an Issuer</p> <p>3.5.1.2, 3.5.1.3 N.A. Tecnes not use disk-level or partition-level encryption</p> <p>3.7.6 N.A. No manual clear-text cryptographic key-management operations are used</p> <p>3.7.9 N.A. because Tecnes doesn't share keys with customers</p> <p>4.2.1.2 N.A. because Tecnes doesn't build wireless networks</p> <p>4.2.2 N.A. because Tecnes, does not use end-user messaging technologies to send CHD</p> <p>8.2.2 N.A. Group, shared, generic IDs, or other shared authentication credentials aren't used.</p> <p>8.2.3 N.A. because Tecnes hasn't remote access to customer environments</p> <p>8.2.5 N.A. because there aren't users terminated In the last six months.</p> <p>8.2.7 N.A. because third parties remote access isn't required.</p> <p>8.3.10 N.A. Tecnes meet Requirement 8.3.10.1.</p> <p>8.3.11 N.A. Authentication factors such as physical or logical security tokens, smart cards, or certificates aren't used</p> <p>8.6.1, 8.6.2 N.A. accounts used by systems or applications can't be used for interactive login,</p> <p>9.4.6 N.A. because Tecnes doesn't have hard-copy materials containing cardholder data</p> <p>9.5 All sub-requirement N.A. because Tecnes doesn't accept card-present transactions</p> <p>11.4.4 N.A. because No exploitable vulnerabilities was found during penetration testing</p> <p>11.4.7 TECNES isn't a Multi-Tenant Service Providers.</p> <p>12.3.2 N.A. Tecnes don't meet any requirement with the customized approach</p> <p>A1 all requirements N.A. TECNES isn't a Multi-Tenant Service Providers</p> <p>A2 all requirements N.A. because Tecnes doesn't collect credit card number using POS POI devices</p> <p>6.4.3,11.6.1 N.A. Future Requirementt</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>Note: This is the first date that evidence was gathered, or observations were made.</i>	2024-07-22
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	2024-11-22
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 2024-11-22)*.

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 TECNES Milano srl 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>(Service Provider Company Name)</i> has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date 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 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>(Service Provider Company Name)</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 border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 35%;">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)

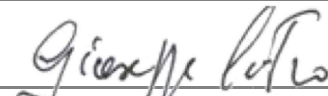
<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the 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.

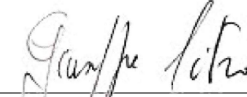
Part 3b. Service Provider Attestation

	
Signature of Service Provider Executive Officer ↑	Date: 2024-11-22
Service Provider Executive Officer Name: Leopoldo Serg	Title: CEO

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: 2024-11-22
Lead QSA Name: Giuseppe Citro	

	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 2024-11-22
Duly Authorized Officer Name: Giuseppe Citro	QSA Company: RISC3 Srl

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:

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/