



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: Mews Systems B.V.

Assessment End Date: June 20, 2024

Date of Report as noted in the Report on Compliance: July 18, 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:	Mews Systems B.V.
DBA (doing business as):	Mews Systems s.r.o
Company mailing address:	Náměstí I. P. Pavlova 5, 120 00 Vinohrady, Czech Republic
Company main website:	https://www.mews.com/
Company contact name:	Jan Taus
Company contact title:	Director of IT and Security
Contact phone number:	+420 737 450 284
Contact e-mail address:	jan.taus@mews.com

Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)

ISA name(s):	Not applicable
--------------	----------------

Qualified Security Assessor

Company name:	Verizon Business Services (hereafter Verizon)
Company mailing address:	H.J.E. Wenckebachweg 123, 1096 AM Amsterdam, The Netherlands
Company website:	http://www.verizonenterprise.com
Lead Assessor name:	David van der Merwe
Assessor phone number:	+31 (0) 655 787 221
Assessor e-mail address:	david.vandermerwe@nl.verizon.com
Assessor certificate number:	007-105

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:	Mews Operations (Commander) version 1858.0.0 Mews Booking Engine (Distributor) version 1338.0.0 Mews Guest Portal (Navigator) version 1353.0.0 Mews Kiosk version 3.12.0
------------------------------	---

Type of service(s) assessed:

Hosting Provider: <input checked="" type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input checked="" type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input checked="" 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 checked="" 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 checked="" type="checkbox"/> Back-Office Services <input checked="" type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider <input type="checkbox"/> Others (specify):	<input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input type="checkbox"/> Merchant Services	<input type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input type="checkbox"/> Tax/Government Payments

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: Not Applicable

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.

Mews does not in any way store, process or transmit cardholder data. It instead integrates a third-party PCI proxy which serves as a tokenization HTTP proxy and which also provides a secure iframe Mews can embed into applications to accept cardholder data. If the payment is done using terminals, Mews sends the request for payment to Adyen. Adyen then communicates with the terminals. Mews is not in touch with any cardholder data from the terminals. Mews uses third party payment gateways (Stripe, Adyen) to

	charge the cards, the communication to Stripe and Adyen is held via PCI proxy which detokenizes the cardholder data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Mews accepts card not present payments through an iFrame embedded in the website and card present payments are managed by the 3rd party payment service providers. Mews also facilitates chargebacks.
Describe system components that could impact the security of account data.	Mews does not in any way store, process or transmit cardholder data. To support their product which is a property management system, they facilitate payment for booking. All the payment page components or terminals come from a third-party PCI DSS compliant service provider. The assessed entity can only impact the security of cardholder data in case the iframe redirection mechanism is compromised.

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.*

Mews use Microsoft Azure as a cloud (PaaS) provider, and utilize the following services (Covered by the Microsoft Azure AoC dated March 07, 2024):

Azure SQL Database for storage of relational data.
 Azure Storage for storage of binary data and system assets.
 Azure Cosmos DB for storage of non-relational data.
 Azure Cache for Redis (remote dictionary server) as caching storage.
 Azure App Service for application hosting.
 Azure DNS for domain management.
 Azure CDN as a content delivery network for images and other assets.
 Azure Traffic Manager for DNS-based load balancing.
 Azure Application Gateway for routing.
 Azure Automation for process automation.
 Azure Application Insights for telemetry.
 Azure Cognitive Services for AI services.

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>
Data center	2	Azure West Central, Germany (Active) Azure East Europe, Ireland (Passive)

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
None	Not Applicable	Not Applicable	Not Applicable	Not Applicable

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

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 checked="" type="checkbox"/> Yes <input 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:
Adyen	Payment Service Provider
Datatrans AG	Token and Payment Service Provider
Microsoft Azure	Cloud Hosting service provider
Stripe	Payment Service 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:

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 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> 1.2.6 - no insecure services and ports 1.5.1 - no user workstations that are able to connect to the CDE 1.3.1, 1.3.2, 1.3.3, 1.4.4 - no CDE in scope 2.2.5 - no insecure services and ports 2.3.1, 2.3.2, 4.2.1.2 - no wireless connections and networks in scope 3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.2, 3.3.3, 3.4.1, 3.4.2, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3, 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, 3.7.8, 3.7.9, 6.5.5 7.2.6, 10.2.1.1, 12.7.1 - CHD and SAD are not stored 4.2.1, 4.2.1.1, 5.2.3.1, 5.4.1, 6.3.2, 6.4.2, 6.4.3, 7.2.4, 7.2.5.1, 8.5.1, 8.6.1, 8.6.2, 8.6.3, 10.4.2.1, 11.3.1.1, 11.3.1.2, 11.3.2.1, 11.5.1.1, 11.6.1, 12.3.1, 12.3.2, 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, 12.10.7 - best practice until 31 March 2025 4.1.1, 4.1.2 - no CHD transmitted 4.2.2 - end user messaging technologies not used 6.2.1, 6.2.2, 6.2.3, 6.2.3.1, 6.2.4, 6.3.2, 6.4.2, - no application development in scope 6.5.2 - no significant changes occurred 8.2.3 - no access to customer premises 8.2.7 - no vendor access 8.3.10, 8.3.10.1, 8.4.1, 8.4.2, 8.4.3, - no access to CHD or CDE 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 - no media containing CHD 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 – no POI device in scope 11.4.7, A1.1.1, A1.1.2, A1.1.3, A1.1.4, A1.2.1, A1.2.2, A1.2.3, A2.1.1, A2.1.2, A2.1.3, A3 - not a Multi-tenant services provider. </p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>None</p>

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

Date Assessment began: Note: This is the first date that evidence was gathered, or observations were made.		2024-05-23
Date Assessment ended: Note: This is the last date that evidence was gathered, or observations were made.		2024-06-20
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 type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
• Examine/observe live data	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
• Observe process being performed	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
• Observe physical environment	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
• Interactive testing	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
• Other:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2024-07-18)*.

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 Mews Systems B.V. 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"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								

Part 3. PCI DSS Validation *(continued)*


Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

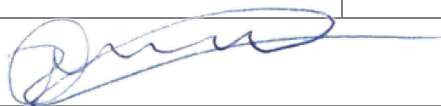
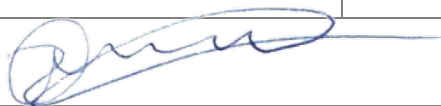
(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.


Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer 		Date: 18th of July 2024
Service Provider Executive Officer Name: Jan Taus		Title: Director of IT and Security

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: July 19, 2024	
Lead QSA Name: David van der Merwe	


 Eric JOLENT (Jul 22, 2024 10:39 GMT+2)

Signature of Duly Authorized Officer of QSA Company 		Date: 22-Jul-2024
Duly Authorized Officer Name: Eric JOLENT		QSA Company: Verizon Business Services

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"/>	

