



# **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: Democrance DMCC**

**Assessment End Date: September 10, 2024**

**Date of Report as noted in the Report on Compliance: September 10, 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:	Democrance DMCC
DBA (doing business as):	NA
Company mailing address:	6 <sup>th</sup> Floor, One JLT, Jumeriah Lake Towers, Dubai, UAE.
Company main website:	<a href="https://www.democrance.com/">https://www.democrance.com/</a>
Company contact name:	Michele Grosso
Company contact title:	CEO
Contact phone number:	97144295831
Contact e-mail address:	<a href="mailto:michele.grosso@democrance.com">michele.grosso@democrance.com</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):	Not Applicable
--------------	----------------

##### Qualified Security Assessor

Company name:	Prescient Security LLC
Company mailing address:	1211 Main Street, Suite 1, Salmon, ID, 83467
Company website:	<a href="https://prescientsecurity.com/">https://prescientsecurity.com/</a>
Lead Assessor name:	Atulkumar Wable
Assessor phone number:	+1 212-271-0175
Assessor e-mail address:	<a href="mailto:pci@prescientsecurity.com">pci@prescientsecurity.com</a>
Assessor certificate number:	PCI DSS QSA, Certificate Number: 206-288



## 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: Payment Facilitator- Insurance Tech Finance Solution

Type of service(s) 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):  
Insurance Tech Finance Solution

☒ 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): None

**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:

#### 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): None

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

Not Applicable

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

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

Democrance utilizes a redirection method provided by the payment service provider (PSP) to collect the card holder data details to complete the authorization of payment card transactions. They receive only the successful or failure message from the payment processor. Democrance utilizes 2C2P, Payfort and Cybersource for providing the payment processing service. The transmission and processing of cardholder data is handled by the payment processor through an HTTPS encrypted channel.



	<p>Democrance does not store any cardholder data information in their environment, so entity will not be having any access to cardholder data once the payment is completed.</p> <p><u>Transmission of CHD</u> Democrance utilizes a redirection method provided by the payment service provider (PSP) to securely collect cardholder data for completing the capture and authorization of transactions. Democrance only receives a success or failure message from the payment processor after the transaction is completed. Democrance contracts with 2C2P, PayFort, and CyberSource for payment processing services. All transmissions to the PSP are through HTTPS encrypted tunnels, ensuring secure communication.</p> <p><u>Processing of CHD</u> All processing of cardholder data transactions was handled by the payment processors.</p> <p><u>Storage of CHD</u> Democrance does not store any cardholder data information in their environment and entity had no access to cardholder data.</p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Democrance is an insurance tech finance solution company which helps their customers by providing a platform to collect payments to purchase policies.
Describe system components that could impact the security of account data.	The primary component of the Democrance systems that impact the security of CHD are the web application services that contain the payment checkout pages. The checkout pages transmit the CHD from the consumer browser session, through the Democrance web application service, and then to the payment gateways for transaction authorization and settlement, as well as tokenization for use in referencing payment methods for future or recurring transactions.



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.

Democrance DMCC (hereafter referred as 'Democrance') is an insurance tech finance solution company which helps their customers by providing a data-enabled SaaS platform that helps insurers and insurance partners to increase digital sales and access new markets. Democrance's platform is constantly evolving to support different personal and commercial insurance products of varying underwriting complexity. Democrance platform's flexibility, coupled with the platform's digital and mobile capabilities, allows insurers to target customers from the high value end all the way down to untapped population segments using one single tool.

Democrance creates value by fully digitizing and automating the entire value chain of insurance from sales to claims management: customers can purchase an insurance product using their phone, while insurance companies can manage the policies through the platform's back end with minimum effort. Democrance has hosted their infrastructure on AWS, Azure and Oracle cloud platform in different regions for their different customers based on their request. Democrance web application is developed and maintained by the internal team.

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)
Amazon Web Services (AWS) (IaaS)	5	N. Virginia, Ireland, Singapore, Africa, UAE
Azure (IaaS)	2	UAE North, Japan East
OCI (IaaS)	1	me-jeddah-1



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<sup>♦</sup>?  
☐ Yes   ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

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





## Part 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 type="checkbox"/> Yes <input checked="" type="checkbox"/> No

### If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services Inc.	Infrastructure as a Service (IaaS)
Google Workspace	SSO
Oracle	Infrastructure as a Service (IaaS)
Microsoft Azure	Infrastructure as a Service (IaaS)
2c2p	Payment Gateway Service Provider
CyberSource	Payment Gateway Service Provider
Payfort	Payment Gateway 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: Payment Facilitator

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 checked="" 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 checked="" 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

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

1.2.6 – Democrance did not support the use of insecure services, protocols, or ports.  
 1.3.3 - Democrance did not support wireless environments that connected to the CDE.  
 1.4.4 - Democrance did not store CHD.

	<p>2.2.5 – Democrance did not support insecure services, daemons, or protocols.</p> <p>2.3.1, 2.3.2 - Democrance did not support wireless environments that connect to the CDE.</p> <p>3.2.1 - Democrance did not directly store CHD.</p> <p>3.3.1 – Democrance did not receive or store SAD.</p> <p>3.3.1.1 - Democrance did not accept full track data as a data variable.</p> <p>3.3.1.2 - CVV was not sent nor stored in the Democrance databases.</p> <p>3.3.1.3 - PIN data couldn't be sent to Democrance.</p> <p>3.3.2 - SAD data was not received by Democrance.</p> <p>3.3.3 - Democrance was not an issuer and did not support issuing services.</p> <p>3.4.1 - Democrance did store CHD and therefore could not display cardholder data.</p> <p>3.4.2 - Democrance had not yet implemented this future dated requirement.</p> <p>3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3, 3.7.1-3.7.9 - Democrance did not directly store CHD.</p> <p>4.2.1.2 - Democrance did not support wireless environments that connect to the CDE.</p> <p>4.2.2 - Democrance did not use end-user messaging technologies to send cardholder data.</p> <p>5.2.3 - All workstations were protected by anti-virus software.</p> <p>5.2.3.1, 5.3.2.1, 5.3.3, 5.4.1 - Democrance had not yet implemented this future dated requirement.</p> <p>6.4.3 - Democrance had not yet implemented this future dated requirement.</p> <p>6.5.2 - Democrance had no significant changes during the assessment period.</p> <p>7.2.6 - Democrance did not directly store CHD.</p> <p>8.2.2 – Democrance did not use shared authentication credentials.</p> <p>8.2.3 - Democrance did not have remote access to customer premises.</p> <p>8.3.10, 8.3.10.1 – Democrance customers were not provided access to account data.</p> <p>8.6.1, 8.6.2, 8.6.3 - This future dated requirement has not yet been implemented.</p> <p>9.4.1-9.4.7 - Democrance did not store CHD in Physical media.</p> <p>9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 - Democrance was not responsible for the management of card reading devices.</p> <p>10.2.1.1 - Democrance did not directly store CHD.</p> <p>11.2.2 - Democrance does not support wireless access points within the cardholder data environment.</p> <p>11.3.1.3, 11.3.2.1 - There were no significant changes to the Democrance system components during the assessment year.</p> <p>11.4.5, 11.4.6 – Democrance did not rely on network segmentation to isolate the CDE.</p> <p>11.4.7 - Democrance clients are not required to perform external penetration testing of the services they use from Democrance.</p> <p>11.5.1.1 - This future dated requirement has not yet been implemented.</p>
--	--



	11.6.1 - Democrance was not responsible for payment page script configuration management. 12.3.2 - Customized approach was not used to meet the PCI DSS requirements. Appendix A1 – Democrance was not considered a multi-tenant service provider. Appendix A2 – Democrance did not support SSL or early TLS.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable



## Section 2 Report on Compliance

### (ROC Sections 1.2 and 1.3.2)

Date Assessment began: <b>Note:</b> This is the first date that evidence was gathered, or observations were made.		07/03/2024
Date Assessment ended: <b>Note:</b> This is the last date that evidence was gathered, or observations were made.		09/10/2024
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 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 September 10, 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 *Democrance DMCC*, 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 *Not applicable* has not demonstrated compliance with PCI DSS requirements.  
**Target Date** for Compliance: *Not applicable*  
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 *Not applicable* 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**


DocuSigned by:  400FF2CE98AE44F...	
Signature of Service Provider Executive Officer ↑	Date: 9/13/2024
Service Provider Executive Officer Name: <b>Michele Grosso</b>	Title: <b>CEO</b>


**Part 3c. Qualified Security Assessor (QSA) Acknowledgement**

If a QSA was involved or assisted with this Assessment, indicate the role performed:

☒ QSA performed testing procedures.☐ QSA provided other assistance.

If selected, describe all role(s) performed:

DocuSigned by:  77F2BEFDC8CF4A0...	
Signature of Lead QSA ↑	Date: 9/13/2024
Lead QSA Name: <b>Atulkumar Wable</b>	

DocuSigned by:  0B32514137D7445...	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 9/13/2024
Duly Authorized Officer Name: <b>Kevin Whalen</b>	QSA Company: <b>Prescient Security LLC</b>

**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"/>	

