



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	Compañía Peruana De Medios De Pago S.A.C.	DBA (doing business as):	Niubiz (former VisaNet Peru)		
Contact Name:	Alfredo Alva	Title:	Infosec Head		
Telephone:	+51 985 908 943	E-mail:	aalva@niubiz.pe		
Business Address:	Av. José Pardo 831 piso 10	City:	Lima		
State/Province:	Lima Province	Country:	Peru	Zip:	15074
URL:	www.niubiz.com.pe				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Foregenix Ltd				
Lead QSA Contact Name:	Leonardo Lima Ferla	Title:	Senior Security Consultant		
Telephone:	+44 845 309 6232	E-mail:	lferla@foregenix.com		
Business Address:	1 Watts Barn	City:	Badbury, Swindon		
State/Province:	Wiltshire	Country:	United Kingdom	Zip:	SN4 0EU
URL:	https://www.foregenix.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed: Acquirer bank (authorization, settlement, chargeback, clearing, back office, monitoring, fraud-prevention, and rewards program)

Type of service(s) assessed:

Hosting Provider:

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web
- Security services
- 3-D Secure Hosting Provider
- Shared Hosting Provider
- Other Hosting (specify):

Managed Services (specify):

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

Payment Processing:

- POS / 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):

Note: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check 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
- Security services
- 3-D Secure Hosting Provider
- Shared Hosting Provider
- Other Hosting (specify):

Managed Services (specify):

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

Payment Processing:

- POS / 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:

Not Applicable

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Compania Peruana de Medios de Pago S.A.C. (Niubiz and formerly VisaNet Peru) is a level 1 service provider located in the city of Lima (Peru).

Compania Peruana de Medios de Pago S.A.C. (Niubiz) is an acquirer bank and is responsible for payment transactions processing (card-present, card-not-present and PIN\Debit) that comes from affiliated merchants. Niubiz also provides other services, such as settlement, chargeback, fraud-prevention, clearing, back-office services (reconciliation, merchant support, incidents, disputes, denied transactions) and a reward program service to merchants.

Niubiz handles cardholder data in the following ways:

Authorization Processing Transactions

Niubiz maintains several authorizations flows but, in general and as part of the authorization process, Niubiz receives card-present and card-not-present transactions from several capture channels such as over the Internet (HTTPS with TLS 1.2 encrypted with AES 256-bit), over private APN (GPRS POS devices), over PSTN lines (Dial-up POS devices) and over private link (payment facilitators). Transactions received contain CHD (Name, PAN and Expiry) and SAD (CV2, Track 2, Track Equivalent Data, PIN-Block). Internally, CHD is transmitted over a local network in clear text.

Transactions received are processed by in-scope applications that are placed in three different places (AWS, IBM Peru, and Telefonica del Peru) and forwarded to the card brand networks (Amex, Diners, Mastercard, UnionPay and Visa) or local bank issuer to be processed by the issuer bank.

For this process, Niubiz handles SAD (CV2, Track 2, Track Equivalent Data, PIN-Block) on several in-scope system components. SAD is handled only in the VRAM and is systematically and automatically purged from the VRAM after the authorization process.

For this process, Niubiz stores CHD (PAN and Expiry) in the following ways:

- Amazon Web Services (AWS): Database
PAN (encrypted with AES 256-bit, truncated with the first 6 and last 4, salted hashed with SHA 256-bit, and tokenized using a random GUID) and Expiry.

- IBM data center: Database
PAN (truncated with the first 6 and last 4).

- Telefonica data center: Files

PAN (in clear-text protect with compensating controls and encrypted with TDES 112-bit, truncated with the first 6 and last 4, encrypted with AES 256-bit (disk encryption)) and Expiry.

Settlement

As part of the settlement process, Niubiz transmits CHD (PAN) over private card brand network (Visa). Internally, CHD is transmitted over a local network using SFTP (encrypted with AES 256-bit). Information received is processed by in-scope applications that are placed in the Telefonica data center.

For this process, Niubiz stores CHD (PAN) in the following ways:

- Telefonica data center: Files
PAN (encrypted with AES 256-bit (disk encryption)).
- Telefonica data center: Database
PAN (encrypted with AES 256-bit (database encryption)).

Chargeback

As part of the chargeback process, Niubiz transmits CHD (PAN) over the Internet (HTTPS with TLS 1.2 encrypted with AES 256-bit). Information received is processed by in-scope applications, that are placed in the Telefonica data center.

For this process, Niubiz stores CHD (PAN) in the following ways:

- Telefonica data center: Database
PAN (encrypted with AES 256-bit (database encryption)).

Clearing

As part of the clearing process, Niubiz transmits CHD (PAN) over a local network using SFTP (encrypted with AES 256-bit). Information received is processed by in-scope applications that are placed in the Telefonica data center.

For this process, Niubiz stores CHD (PAN) in the following ways:

- Telefonica data center: Files

PAN (in clear-text protected with compensating controls and encrypted with TDES 112-bit, encrypted with AES 256-bit (disk encryption)).

- Telefonica data center: Database
PAN (encrypted with AES 256-bit (database encryption)).

Back-Office Services

Niubiz maintains several back-office flows but, in general and as part of the back-office process, Niubiz transmits CHD (PAN and Expiry) from several channels such as over the Internet (HTTPS with TLS 1.2 encrypted with AES 256-bit and secure email encrypted with AES 256-bit), over the local network using SFTP (encrypted with AES 256-bit) and over the local network using HTTPS (TLS 1.2 encrypted with AES 256-bit). Information received is processed by in-scope applications, that are placed in two different data centers (IBM Peru and Telefonica del Peru).

For this process, Niubiz stores CHD (PAN and Expiry) in the following ways:

- Telefonica data center: File
PAN (in clear-text protected with compensating controls and encrypted with TDES 112-bit, encrypted with AES 256-bit (disk encryption), truncated with the first 6 and last 4).
- Telefonica data center: Secure email
PAN encrypted with AES 256-bit (secure email).
- Telefonica data center: Database
PAN (encrypted with AES 256-bit (database encryption) truncated with the first 6 and last 4)).

Monitoring (NOC)

As part of the monitoring (NOC) process, Niubiz transmits CHD (PAN) over a local network using SFTP (encrypted with AES 256-bit) between in-scope system components. Information transmitted is processed by in-scope applications, that are placed in two different data centers (IBM Peru and Telefonica del Peru).

For this process, Niubiz stores CHD (PAN and Expiry) in the following ways:

- Telefonica data center: Files
PAN (encrypted with AES 256-bit (disk encryption)).

	<ul style="list-style-type: none"> • Telefonica data center: Database PAN (encrypted with AES 256-bit (database encryption)). <p>Fraud-Prevention</p> <p>As part of the fraud-prevention process, Niubiz transmits CHD (PAN) over the Internet (secure email encrypted with AES 256-bit) and receives transactions with PAN from other in-scope systems (such as transactional switch and other web applications) over a local network. Information transmitted is processed by in-scope applications, that are placed in Telefonica data center.</p> <p>For this process, Niubiz stores CHD (PAN) in the following ways:</p> <ul style="list-style-type: none"> • Telefonica data center: Secure email PAN (encrypted with AES 256-bit (secure email)). • Telefonica data center: Database PAN (encrypted with TDES 168-bit and hashed with SHA 256-bit (only stores the first hash 20-digits)). • Telefonica data center: Files Not valid PAN (encrypted with AES 256-bit (disk encryption)). <p>Reward Program</p> <p>As part of the fraud-prevention process, Niubiz transmits CHD (PAN) over the Internet (HTTPS with TLS 1.2 encrypted with AES 256-bit and VPN IPsec Site-To-Site encrypted with AES 256-bit) and over private APN (GPRS POS devices). Information transmitted is processed by in-scope applications that are placed in AWS data center.</p> <p>For this process, Niubiz stores CHD (PAN) in the following ways:</p> <ul style="list-style-type: none"> • AWS: Tables PAN truncated with the first 6 and last 4
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p>Not Applicable</p>

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Data Center	4	Lima/Peru
Data Center (Cloud Computing)	2	Virginia/United Stated
Office	1	Lima/Peru
Offsite storage	3	Lima/Peru

Part 2d. Payment Application

Does the organization use one or more Payment Applications? Yes No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
VNP Stratus	1.0	Not Applicable	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Not Applicable

Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.

The scope of the assessment consists of personnel, processes and technologies located in 4 on-premises data centers (IBM and Telefonica), 2 cloud-computing data centers (AWS) and 1 corporate office, where the following technologies are implemented.

- Asymmetric encryption keys (RSA)
- Authoritative database (LDAP)
- Change management ticket system.
- Database
- Database services (PaaS)
- Custom payment applications
- Disk encryption technology
- File Integrity Monitoring (FIM)
- File encryption technology
- Hash algorithms (SHA)
- Host Intrusion Detection System (HIDS)
- HSM (Hardware Security Module)
- IaaS technologies provided by AWS.
- Linux Operating Systems
- Log aggregation solution
- Network switches

- PaaS technologies provided by AWS.
- Private links
- Stateful firewalls
- Stateful firewalls (PaaS)
- Secure Code tool
- Symmetric encryption algorithms
- Software OTP solution
- Table encryption technology
- TLS connections
- VPN solution
- Vulnerability scanner solution
- Web application servers
- Web Application Firewall (WAF) solution
- Windows OS Operating Systems
- Virtualization platform

Also, connections in and out with CDE are placed according below:

Card Brand connections

Amex, Diners, Mastercard:

Indirectly connected over service provider

UnionPay and Visa:

Directly connected over private links (MPLS).

Data Center connections

AWS (management portal):

Indirectly connected over the Internet using a secure channel for technical reasons.

IBM:

Directly connected over private links with Telefonica and Niubiz office.

Directly connected with contingency site via dark fiber.

Directly connected over private links with BANCA RED (issuer).

Directly connect over the Internet using a VPN IPsec Site-To-Site with AWS.

Telefonica:

Directly connected over private links with Telefonica and Niubiz office.

	<p>Directly connected with contingency site via dark fiber.</p> <p>Directly connected over private links with BANCA RED (issuers network).</p> <p>Directly connect over the Internet using a VPN IPsec Site-To-Site with AWS.</p> <p>Directly connect over private links with Visa Inc.</p> <p>Other connections</p> <p>Bank issuers:</p> <p>Directly connected over private links (MPLS) via VRFs segments. Connection between Telefonica data center and issuers banks.</p>
--	--

<p>Does your business use network segmentation to affect the scope of your PCI DSS environment? <i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i></p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
--	---

Part 2f. Third-Party Service Providers

<p>Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?</p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
--	---

If Yes:

Name of QIR Company:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable

<p>Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?</p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
--	---

If Yes:

Name of service provider:	Description of services provided:
Amazon Web Services (AWS)	Cloud computing services
CyberSource	Transaction scoring & 3DS service
IBM Peru	Hosting and management services
Invenio	ISO file conversion
Iron Mountain	Offsite backup storage service provider
Italtel	Asset management
NeoSecure	SOC
Orion	Cloud management services
Procesos MC	Amex and Mastercard processing
SecureSoft	Load balancer management

Telefonica del Peru	Hosting and management services
Unibanca	Diner's processing

Note: Requirement 12.8 applies to all entities in this list.

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

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:		Acquirer bank (authorization, settlement, chargeback, clearing, back office, monitoring, fraud-prevention and rewards program)		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 1.2.2: No routers in-scope
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 2.1.1: No wireless networks in-scope 2.2.3: No insecure protocols in-scope 2.6: Niubiz is not a Shared Hosting Provider
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 3.6: No encryption keys are shared 3.6.6: No clear-text keys in-scope
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 4.1.1: No wireless networks in-scope

Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 6.4.6: No significant changes past 12 months in-scope
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 8.1.5: No temporary access to service providers 8.5.1: No access to customer premises
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 9.8.1: No hard-copy media with CHD in-scope 9.9, 9.9.1, 9.9.2, 9.9.3: No POI devices in-scope
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 11.2.3: No significant changes past 12 months in-scope 11.3.3: No exploitable vulnerabilities found.
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable 12.3.9: No remote access activation technologies in-scope

Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable A1.X: Niubiz is not a Shared Hosting Provider
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable A.2.1: No POI devices in-scope A.2.2: No SSL/TLS early in-scope A.2.3: No SSL/TLS early in-scope

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	14 Mar 2023
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 14 Mar 2023.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (**check one**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby Compañía Peruana De Medios De Pago S.A.C. has demonstrated full compliance with the PCI DSS.</p>				
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>				
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more requirements are marked “Not in Place” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th style="width: 50%;">Affected Requirement</th> <th style="width: 50%;">Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td style="height: 40px;"></td> <td></td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met		
Affected Requirement	Details of how legal constraint prevents requirement being met				

Part 3a. Acknowledgement of Status

Signatory(s) confirms:


(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, 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 my assessment in all material respects.
<input checked="" type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)

<input checked="" type="checkbox"/>	No evidence of full track data ¹ , CAV2, CVC2, CID, or CVV2 data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Trustwave

Part 3b. Service Provider Attestation



<i>Signature of Service Provider Executive Officer</i> ↑	<i>Date:</i> 14 Mar 2023
<i>Service Provider Executive Officer Name:</i> Alfredo Alva	<i>Title:</i> Infosec head

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	Foregenix assessor (Leonardo Lima Ferla) performed the physical assessment, validated evidence such as process, documents and technical configurations and is responsible for the ROC.
--	--

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i> 14 Mar 2023
<i>Duly Authorized Officer Name:</i> Leonardo Lima Ferla	<i>QSA Company:</i> Foregenix Ltd

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Not Applicable
---	----------------

¹ Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

² The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

³ Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" 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 checked="" type="checkbox"/>	<input type="checkbox"/>	

