



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: | Intuit Inc. | DBA (doing business as): | QuickBooks Online Payments (QBO Payments) Intuit Processor Intuit Canada ULC Intuit UK Limited Intuit Inc. – Innovative Merchants Solutions, LLC. Intuit Payment Solutions, LLC | | |
| Contact Name: | David Martin | Title: | Technical Compliance and Audit Manager | | |
| Telephone: | +1 858.753.5994 | E-mail: | david_martin@intuit.com | | |
| Business Address: | 21650 W. Oxnard St Suite 2200 | City: | Woodland Hills | | |
| State/Province: | CA | Country: | USA | Zip: | 91367 |
| URL: | https://www.intuit.com | | | | |

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

| | | | | | |
|------------------------|--|----------|-------------------|------|-------|
| Company Name: | Tevora Business Solutions, Inc. (DBA Tevora) | | | | |
| Lead QSA Contact Name: | Bill Nguyen | Title: | Associate Manager | | |
| Telephone: | +1 949.250.3290 | E-mail: | qsa@tevora.com | | |
| Business Address: | 17875 Von Karman Ave #100 | City: | Irvine | | |
| State/Province: | CA | Country: | USA | Zip: | 92614 |
| URL: | https://www.tevora.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: QuickBooks Online Payments

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: | Turbo Tax, Canada Turbo Tax Online, QuickBooks Desktop, QuickBooks Point of Sale, Mint, Intuit Online Payroll, Intuit Enterprise Payment Services, Financial Data Services Aggregation, Intuit Tax Data Import and Upload, Enterprise Security Services, Intuit Core Services, and any other Intuit business unit or service that may be in scope for PCI |
|----------------------------------|---|

Type of service(s) not assessed:

| | | |
|--|---|---|
| <p>Hosting Provider:</p> <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 checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify): | <p>Managed Services (specify):</p> <input checked="" type="checkbox"/> Systems security services <input checked="" type="checkbox"/> IT support <input checked="" type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify): | <p>Payment Processing:</p> <input checked="" type="checkbox"/> POS / card present <input checked="" type="checkbox"/> Internet / e-commerce <input checked="" type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify): |
| <input checked="" type="checkbox"/> Account Management | <input checked="" type="checkbox"/> Fraud and Chargeback | <input checked="" type="checkbox"/> Payment Gateway/Switch |
| <input checked="" type="checkbox"/> Back-Office Services | <input checked="" type="checkbox"/> Issuer Processing | <input type="checkbox"/> Prepaid Services |
| <input checked="" 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): | | |

| | |
|---|--|
| Provide a brief explanation why any checked services were not included in the assessment: | Intuit, Inc. conducts separate PCI DSS assessments for its various services. QBO Payments is the scope of this assessment. |
|---|--|

Part 2b. Description of Payment Card Business

| | |
|---|---|
| <p>Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.</p> | <p>Intuit's QuickBooks Online Payments ("QBO Payments") is a business unit within Intuit that provides services pertaining to payment authorization, transaction lifecycle management, data security services, customer relationship management, and cash card lifecycle management. QBO Payments provides the following services:</p> <p>Wallet is a sensitive data tokenization service, providing both tokenizing and detokenizing functions. Wallet also provides the capability to temporarily store sensitive authentication data (SAD), disposing of SAD after first use. API calls containing CHD are made to the Wallet service via TLS 1.2, and CHD is stored</p> |
|---|---|

hashed and encrypted within the Wallet service database.

Wallet Cash is a service that manages the lifecycle of QuickBooks Cash Debit Cards. API calls containing CHD are made to the Wallet Cash service via TLS 1.2, and the Wallet Cash service exchanges CHD with the Wallet Service and its partner card issuing entities via TLS 1.2.

Mobile is a service that handles transactions received via Intuit's QuickBooks Mobile point-of-sale application endpoints. API calls containing CHD are made to the Mobile services via TLS 1.2, and the Mobile service exchanges CHD with the Wallet Service and the PayAPI services via TLS 1.2.

Payment API/PayAPI/Auth is a service that provides transaction authorization services. PayAPI receives API calls containing CHD over TLS 1.2. PayAPI exchanges CHD with Intuit Data Protection Services (IDPS), Wallet Service, Payment Processors, and the "Authorization Queue" via TLS 1.2. PayAPI uses IDPS to hash and encrypt CHD and stores these hashed and encrypted values within the PayAPI database. PayAPI also receives tokenized CHD, which it exchanges with the Wallet Service to retrieve CHD for subsequent authorization flows.

Payments Workflow is a service that provides a simplified interface that orchestrates PayAPI and T360 services. Payments Workflow only receives and transmits tokenized CHD to coordinate subsequent authorization and transaction lifecycle management workflows.

Transaction 360/T360 is a service that ensures the capture, recording, and preservation of transaction data. T360 receives CHD from the "Authorization Queue" via TLS 1.2. T360 encrypts and hashes CHD using the IDPS service and stores the resulting values within the T360 database.

Instant Transfer is a service that supports a customer "Instant Transfer" request, where funds from invoices may be immediately deposited into the customer account. The Instant Transfer services receives tokens, which it passes to the Wallet Services in exchange for CHD via TLS 1.2. The Instant Transfer service then sends this data to VisaDirect using VISA APIs.

| | |
|--|---|
| | <p>Dispute is a collection of services that support collections and exceptions process including chargebacks. Dispute reads CHD from T360 and OASIS to display dispute details via the iBoss interface.</p> <p>Agent PCI Service is an applet used by Intuit agents to retrieve CHD. Agent PCI Service reads CHD from T360 to display card details via the iBoss interface.</p> |
| Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data. | Not Applicable. All security impacting elements have been described above. |

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): |
|--|-----------------------------------|--|
| Corporate Headquarters | 1 | Woodland Hills, California, USA |
| Amazon Web Services Availability Regions | 2 | us-east-2: Oregon, USA us-west-2: Ohio, USA |

Part 2d. Payment Applications

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) |
|--------------------------|----------------|--------------------|--|--|
| Not Applicable | Not Applicable | Not Applicable | <input type="checkbox"/> Yes <input 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.

This assessment covered the QBO Payments production AWS VPCs and the in-scope applications hosted therein, i.e., Wallet, Wallet Cash, Mobile, Payment API/PayAPI/Auth, Payments Workflow, Transaction 360/T360, Instant Transfer, Dispute, and Agent PCI Service.

Infrastructure elements reviewed as part of this assessment included the AWS networking configurations of VPCs managed by the QBO Payments team.

System components reviewed as part of this assessment include the applications developed by QBO Payments, the EC2 instances residing within the data-tier subnets, and the databases that store CHD.

Connections into and out of the QBO Payments CDE includes connections to various banking entities, payment processors, and API calls with other services within Intuit.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

Yes No

Part 2f. Third-Party Service Providers

| | |
|---|---|
| Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated? | <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 |

| | |
|---|---|
| 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? | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
|---|---|

If Yes:

| Name of service provider: | Description of services provided: |
|--|--|
| Amazon Web Services, LLC | IT Shared Services Hosting |
| PayPal Holdings, LLC | Financial Transaction and Account Services |
| JP Morgan Chase & CO | Financial Transaction and Account Services |
| American Express Company | Financial Transaction and Account Services |
| Merchant Link LLC. | Financial Transaction and Account Services |
| Intuit Data Protection Services (IDPS) | Data Encryption and Protection Services |
| Intuit Inc. (Enterprise Security Services) | Managed Infrastructure and Security Services |
| Intuit Inc. (Core Services) | Managed Infrastructure and Platform Service |

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: | | QuickBooks Online Payments | | |
|---------------------------|-------------------------------------|-------------------------------------|--------------------------|--|
| 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 checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 2: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 2.1.1: Not applicable; QBO Payments does not use wireless technology within the in-scope environment. 2.2.3: Not applicable; QBO Payments does not enable insecure services. 2.6: Not applicable; QBO Payments is not a shared hosting provider. |
| Requirement 3: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 3.4.1: Not applicable; QBO Payments does not use disk encryption. 3.6: Not applicable; QBO Payments does not share encryption keys with customers. 3.6.6: Not applicable; QBO Payments does not use manual clear-text cryptographic key-management operations. |
| Requirement 4: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 4.1.1: Not applicable; QBO payments does not use any wireless technology within the in-scope environment. 4.2.a: Not applicable; QBO Payments does not use end-user messaging technologies to send cardholder data. |
| Requirement 5: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 6: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 7: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

| | | | | |
|-----------------|-------------------------------------|-------------------------------------|-------------------------------------|---|
| Requirement 8: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <p>8.1.5: Not applicable; QBO Payments does not permit vendor access into the cardholder data environment.</p> <p>8.2.1.d: Not applicable; QBO Payments does not provision non-customer consumers with access to in-scope systems.</p> <p>8.2.1.e: Not applicable; QBO Payments does not provision non-customer consumers with access to in-scope systems.</p> <p>8.2.3.b: Not applicable; QBO Payments does not provision non-customer consumers with access to in-scope systems.</p> <p>8.2.4.b: Not applicable; QBO Payments does not provision non-customer consumers with access to in-scope systems.</p> <p>8.2.5.b: Not applicable; QBO Payments does not provision non-customer consumers with access to in-scope systems.</p> <p>8.5.1: Not applicable; QBO Payments does not have remote access to customer environments.</p> |
| Requirement 9: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <p>9.5: Not applicable; QBO Payments does not store CHD on media.</p> <p>9.6: Not applicable; QBO Payments does not store CHD on media.</p> <p>9.7: Not applicable; QBO Payments does not store CHD on media.</p> <p>9.8: Not applicable; QBO Payments does not store CHD on media.</p> <p>9.9: Not applicable; QBO Payments does not maintain POS/POI devices.</p> |
| Requirement 10: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 11: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 12: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Appendix A1: | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Appendix A2: | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |

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: | 21 Jul 2022 | |
| Have compensating controls been used to meet any requirement in the ROC? | <input type="checkbox"/> Yes | <input checked="" 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 21 Jul 2022.

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 Intuit, Inc. 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>Not Applicable</i> has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance: Not Applicable</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 your acquirer or 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%;"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Not Applicable</td> <td style="text-align: center;">Not Applicable</td> </tr> </tbody> </table> | Affected Requirement | Details of how legal constraint prevents requirement being met | Not Applicable | Not Applicable |
| Affected Requirement | Details of how legal constraint prevents requirement being met | | | | |
| Not Applicable | Not Applicable | | | | |

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, Version 3.2.1</i> , 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 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 <i>SecurityMetrics</i> |

Part 3b. Service Provider Attestation

| | |
|---|---|
|  | |
| Signature of Service Provider Executive Officer ↑ | Date: 27 Jul 22 |
| Service Provider Executive Officer Name: David Martin | Title: Technical Compliance and Audit Manager |

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

| | |
|--|---|
| If a QSA was involved or assisted with this assessment, describe the role performed: | <i>The QSA performed remote assessment activities, validation of controls, and review of documentation including policies, procedures, standards, vendor documentation, and configuration settings.</i> |
|--|---|

| | |
|--|---------------------|
|  | |
| Signature of Duly Authorized Officer of QSA Company ↑ | Date: 28 Jul 2022 |
| Duly Authorized Officer Name: Bill Nguyen | QSA Company: Tevora |

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: | Hussain Jawadwala: Project management, resource allocation and coordination, provided requested evidence and documents. Rick Slater: Provided requested evidence and documents. |
|---|--|

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 type="checkbox"/> | <input checked="" type="checkbox"/> | Not Applicable |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Not Applicable |

