Questionnaire SAQ D

Build and Maintain a Secure Network and Systems Completed
Protect Cardholder Data Completed
Maintain a Vulnerability Management Program Completed
Implement Strong Access Control Measures Completed
Regularly Monitor and Test Networks Completed
Maintain an Information Security Policy Completed

Build and Maintain a Secure Network and Systems

Install and maintain a firewall configuration to protect cardholder data

1.1

Are firewall and router configuration standards established and implemented to include the following:

1.1.1 *Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.1.2(a) *Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.1.2(b) *Is there a process to ensure the diagram is kept current?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.1.3(a) *Is there a current diagram that shows all cardholder data flows across systems and networks?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.1.3(b) *Is there a process to ensure the diagram is kept current?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.1.4(a) *Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.1.4(b) *Is the current network diagram consistent with the firewall configuration standards?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.1.5 *Are groups, roles, and responsibilities for logical management of network components assigned and documented in the firewall and router configuration standards?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.1.6(a) *Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.1.6(b) *Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.1.7(a) *Do firewall and router configuration standards require review of firewall and router rule sets at least every six months?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

1.1.7(b) *Are firewall and router rule sets reviewed at least every six months?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

1.2

Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows:

Note: *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*

1.2.1(a) *Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.2.1(b) *Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.2.2 *Are router configuration files secured from unauthorized access and synchronized - for example, the running (or active) configuration matches the start-up configuration (used when machines are booted)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.2.3 *Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to the use of wireless technology and only needs to be answered if such technology is present anywhere in your network. You have indicated in your profile that you do not use wireless technology in your network.

1.3 Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:

1.3.1 *Is a DMZ implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.3.2 *Is inbound Internet traffic limited to IP addresses within the DMZ?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.3.3 *Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network?*

(For example, block traffic originating from the internet with an internal address.)

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.3.4 *Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.3.5 *Are only established connections permitted into the network?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.3.6 *Are system components that store cardholder data (such as a database) placed in an internal network zone, segregated from the DMZ and other untrusted networks?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

1.3.7(a) *Are methods in place to prevent the disclosure of private IP addresses and routing information to the Internet?*

Note: *Methods to obscure IP addressing may include, but are not limited to:*

- *Network Address Translation (NAT)*
- *Placing servers containing cardholder data behind proxy servers/firewalls,*
- *Removal or filtering of route advertisements for private networks that employ registered addressing,*
- *Internal use of RFC1918 address space instead of registered addresses.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.3.7(b) *Is any disclosure of private IP addresses and routing information to external entities authorized?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.4(a) *Is personal firewall software (or equivalent functionality) installed and active on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.4(b) *Is the personal firewall software (or equivalent functionality) configured to specific configuration settings, actively running, and not alterable by users of mobile and/or employee-owned devices?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

1.5 *Are security policies and operational procedures for managing firewalls:*

- *Documented*
- *In use*
- *Known to all affected parties?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Do not use vendor-supplied defaults for system passwords and other security parameters

2.1(a) *Are vendor-supplied defaults always changed before installing a system on the network?*

This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.1(b) *Are unnecessary default accounts removed or disabled before installing a system on the network?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:

2.1.1(a) *Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to the use of wireless technology and only needs to be answered if such technology is present anywhere in your network. You have indicated in your profile that you do not use wireless technology in your network.

2.1.1(b) *Are default SNMP community strings on wireless devices changed at installation?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to the use of wireless technology and only needs to be answered if such technology is present anywhere in your network. You have indicated in your profile that you do not use wireless technology in your network.

2.1.1(c) *Are default passwords/passphrases on access points changed at installation?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to the use of wireless technology and only needs to be answered if such technology is present anywhere in your network. You have indicated in your profile that you do not use wireless technology in your network.

2.1.1(d) *Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to the use of wireless technology and only needs to be answered if such technology is present anywhere in your network. You have indicated in your profile that you do not use wireless technology in your network.

2.1.1(e) *Are other security-related wireless vendor defaults changed, if applicable?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to the use of wireless technology and only needs to be answered if such technology is present anywhere in your network. You have indicated in your profile that you do not use wireless technology in your network.

2.2(a) *Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards?*

Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2(b) *Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2(c) *Are system configuration standards applied when new systems are configured?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2(d) *Do system configuration standards include all of the following:*

- *Changing of all vendor-supplied defaults and elimination of unnecessary default accounts?*
- *Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server?*
- *Enabling only necessary services, protocols, daemons, etc., as required for the function of the system?*

- *Implementing additional security features for any required services, protocols or daemons that are considered to be insecure?*
- *Configuring system security parameters to prevent misuse?*
- *Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.1(a) *Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server?*

For example, web servers, database servers, and DNS should be implemented on separate servers.

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.1(b) *If virtualization technologies are used, is only one primary function implemented per virtual system component or device?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.2(a) *Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.2(b) *Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.3 *Are additional security features documented and implemented for any required services, protocols or daemons that are considered to be insecure?*

Note: *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.4(a) *Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.4(b) *Are common system security parameters settings included in the system configuration standards?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.4(c) *Are security parameter settings set appropriately on system components?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.5(a) *Has all unnecessary functionality such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers been removed?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.5(b) *Are enabled functions documented and do they support secure configuration?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

2.2.5(c) *Is only documented functionality present on system components?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

2.3

Is non-console administrative access encrypted as follows:

Note: *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed*

2.3(a)

Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

2.3(b)

Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

2.3(c)

Is administrator access to web-based management interfaces encrypted with strong cryptography?

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

2.3(d)

For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

2.4(a)

Is an inventory maintained for systems components that are in scope for PCI DSS, including a list of hardware and software components and a description of function /use for each?

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

2.4(b) *Is the documented inventory kept current?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

2.5 *Are security policies and operational procedures for managing vendor defaults and other security parameters:*

- *Documented*
- *In use*
- *Known to all affected parties?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Protect Cardholder Data

Protect stored cardholder data

3.1 Are data-retention and disposal policies, procedures, and processes implemented as follows:

3.1(a) *Is data storage amount and retention time limited to that required for legal, regulatory, and/or business requirements?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.1(b) *Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, and/or business reasons?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.1(c) *Are there specific retention requirements for cardholder data?*

For example, cardholder data needs to be held for X period for Y business reasons.

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.1(d) *Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

3.1(e) *Does all stored cardholder data meet the requirements defined in the data-retention policy?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.2(c) *Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.2(d)

Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

3.2.1 *The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored after authorization?This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.*

Note: *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:*

- *The cardholder's name,*
- *Primary account number (PAN),*
- *Expiration date, and*
- *Service code*

To minimize risk, store only these data elements as needed for business.

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.2.2 *The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.2.3 *The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.3 *Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN?*

Note: *This requirement does not supersede stricter requirements in place for displays of cardholder data for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.4 *Is PAN rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs), by using any of the following approaches?*

- *One-way hashes based on strong cryptography (hash must be of the entire PAN)*
- *Truncation (hashing cannot be used to replace the truncated segment of PAN)*
- *Index tokens and pads (pads must be securely stored)*
- *Strong cryptography with associated key management processes and procedures.*

Note: *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.4.1 If disk encryption (rather than file- or column-level database encryption) is used, is access managed as follows:

Note: *This requirement applies in addition to all other PCI DSS encryption and key management requirements.*

3.4.1(a) *Is logical access to encrypted file systems managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.4.1(b) *Are cryptographic keys stored securely (for example, stored on removable media that is adequately protected with strong access controls)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.4.1(c) *Is cardholder data on removable media encrypted wherever stored?*

Note: *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.5

Are keys used to secure stored cardholder data protected against disclosure and misuse as follows:

Note: *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys. Such key-encrypting keys must be at least as strong as the data-encrypting key.*

3.5.2 *Is access to cryptographic keys restricted to the fewest number of custodians necessary?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.5.3 *Are secret and private cryptographic keys used to encrypt/decrypt cardholder data stored in one (or more) of the following forms at all times?*

- *Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key*
- *Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)*
- *As at least two full-length key components or key shares, in accordance with an industry-accepted method.*

Note:*It is not required that public keys be stored in one of these forms.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.5.4 *Are cryptographic keys stored in the fewest possible locations?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.6(a) *Are all key-management processes and procedures fully documented and implemented for cryptographic keys used for encryption of cardholder data?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.6(c)

Are key-management processes and procedures implemented to require the following:

3.6.1 *Do cryptographic key procedures include the generation of strong cryptographic keys?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.6.2 *Do cryptographic key procedures include secure cryptographic key distribution?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.6.3 *Do cryptographic key procedures include secure cryptographic key storage?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.6.4 *Do cryptographic key procedures include cryptographic key changes for keys that have reached the end of their defined cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.6.5(a) *Do cryptographic key procedures include retirement or replacement (for example, archiving, destruction, and/or revocation) of cryptographic keys when the integrity of*

the key has been weakened (for example, departure of an employee with knowledge of a clear-text key)?

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.6.5(b) *Do cryptographic key procedures include replacement of known or suspected compromised keys?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.6.5(c) *If retired or replaced cryptographic keys are retained, are these keys only used for decryption/verification purposes, and not used for encryption operations?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.6.6 *If manual clear-text key-management operations are used, do cryptographic key procedures include split knowledge and dual control of cryptographic keys as follows:*

Do split knowledge procedures require that key components are under the control of at least two people who only have knowledge of their own key components?

AND

Do dual control procedures require that at least two people are required to perform any key management operations and no one person has access to the authentication materials (for example, passwords or keys) of another?

Note: *Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.6.7 *Do cryptographic key procedures include the prevention of unauthorized substitution of cryptographic keys?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

3.6.8 *Are cryptographic key custodians required to formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

3.7 *Are security policies and operational procedures for protecting stored cardholder data:*

- *Documented*
- *In use*
- *Known to all affected parties?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Encrypt transmission of cardholder data across open, public networks

4.1(a) *Are strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks?*

Note: *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*

Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

4.1(b) *Are only trusted keys and/or certificates accepted?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

4.1(c) *Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

4.1(d) *Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

4.1(e) *For TLS implementations, is TLS enabled whenever cardholder data is transmitted or received?*

For example, for browser-based implementations:

- *"HTTPS" appears as the browser Universal Record Locator (URL) protocol, and*
- *Cardholder data is only requested if "HTTPS" appears as part of the URL.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

4.1.1 *Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to the use of wireless technology and only needs to be answered if such technology is present anywhere in your network. You have indicated in your profile that you do not use wireless technology in your network.

4.2(a) *Are PANs rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

4.2(b) *Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

4.3 *Are security policies and operational procedures for encrypting transmissions of cardholder data:*

- *Documented*
- *In use*
- *Known to all affected parties?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Maintain a Vulnerability Management Program

Protect all systems against malware and regularly update anti-virus software or programs

5.1 *Is anti-virus software deployed on all systems commonly affected by malicious software?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

5.1.1 *Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

5.1.2 *Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

5.2

Are all anti-virus mechanisms maintained as follows:

5.2(a) *Are all anti-virus software and definitions kept current?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

5.2(b) *Are automatic updates and periodic scans enabled and being performed?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

5.2(c) *Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

5.3 *Are all anti-virus mechanisms:*

- *Actively running?*
- *Unable to be disabled or altered by users?*

Note: *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

5.4 *Are security policies and operational procedures for protecting systems against malware:*

- *Documented*

- *In use*
- *Known to all affected parties?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Develop and maintain secure systems and applications

6.1 *Is there a process to identify security vulnerabilities, including the following:*

- *Using reputable outside sources for vulnerability information?*
- *Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities?*

Note: *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.*
Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.2(a) *Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.2(b) *Are critical security patches installed within one month of release?*

Note: *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.3(a) *Are software- development processes based on industry standards and/or best practices?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.3(b) *Is information security included throughout the software-development life cycle?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.3(c) *Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.3(d) Do software development processes ensure the following at 6.3.1 - 6.3.2:

6.3.1 *Are development, test, and/or custom application accounts, user IDs, and passwords removed before applications become active or are released to customers?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.3.2 *Is all custom code reviewed prior to release to production or customers to identify any potential coding vulnerability (using either manual or automated processes) as follows:*

- *Are code changes reviewed by individuals other than the originating code author, and by individuals who are knowledgeable about code review techniques and secure coding practices?*
- *Do code reviews ensure code is developed according to secure coding guidelines?*
- *Are appropriate corrections implemented prior to release?*
- *Are code review results reviewed and approved by management prior to release?*

Note: *This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can*

be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.4

Are change control processes and procedures followed for all changes to system components to include the following:

6.4.1(a)

Are development/test environments separate from the production environment?

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.4.1(b)

Is access control in place to enforce the separation between the development/test environments and the production environment?

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.4.2

Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.4.3

Are production data (live PANs) not used for testing or development?

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.4.4

Are test data and accounts removed from system components before the system becomes active / goes into production?

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.4.5(a) *Are change-control procedures documented and require the following?*

- *Documentation of impact*
- *Documented change control approval by authorized parties*
- *Functionality testing to verify that the change does not adversely impact the security of the system*
- *Back-out procedures*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.4.5(b) Are the following performed and documented for all changes:

6.4.5.1 *Documentation of impact?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.4.5.2 *Documented approval by authorized parties?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.4.5.3 (a) *Functionality testing to verify that the change does not adversely impact the security of the system?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.4.5.3 (b) *For custom code changes, testing of updates for compliance with PCI DSS Requirement 6.5 before being deployed into production?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.4.5.4 *Back-out procedures?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.4.6 *Upon completion of a significant change, are all relevant PCI DSS requirements implemented on all new or changed systems and networks, and documentation updated as applicable?*

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. If / when you are compliant with this requirement, please change your answer to yes.

6.5(a) *Do software-development processes address common coding vulnerabilities?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.5(b) *Are developers trained at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

6.5(c)

Are applications developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities:

Note: *The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the Open Web Application Security Project (OWASP) Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*

6.5.1 *Do coding techniques address injection flaws, particularly SQL injection?*

Note: *Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.5.2 *Do coding techniques address buffer overflow vulnerabilities?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.5.3 *Do coding techniques address insecure cryptographic storage?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.5.4 *Do coding techniques address insecure communications?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.5.5 *Do coding techniques address improper error handling?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.5.6 *Do coding techniques address all "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

For web applications and application interfaces (internal or external), are applications developed based on secure coding guidelines to protect applications from the following additional vulnerabilities:

6.5.7 *Do coding techniques address cross-site scripting (XSS) vulnerabilities?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.5.8 *Do coding techniques address improper access control such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.5.9 *Do coding techniques address cross-site request forgery (CSRF)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.5.10 *Do coding techniques address broken authentication and session management?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

6.6 *For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying either of the following methods?*

Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows:

- *At least annually*
- *After any changes*
- *By an organization that specializes in application security*
- *That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment*
- *That all vulnerabilities are corrected*
- *That the application is re-evaluated after the corrections*

Note: *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.*

- OR -

Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) as follows:

- *Is situated in front of public-facing web applications to detect and prevent web-based attacks.*
- *Is actively running and up to date as applicable.*
- *Is generating audit logs.*
- *Is configured to either block web-based attacks, or generate an alert that is immediately investigated.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

6.7 *Are security policies and operational procedures for developing and maintaining secure systems and applications:*

- *Documented*
- *In use*
- *Known to all affected parties?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Implement Strong Access Control Measures

Restrict access to cardholder data by business need to know

7.1

Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:

7.1

Is there a written policy for access control that incorporates the following?

- *Defining access needs and privilege assignments for each role*
- *Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities,*
- *Assignment of access based on individual personnel's job classification and function*
- *Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved*

[X] Yes [ ] No [ ] N/A

7.1.1

Are access needs for each role defined, including:

- *System components and data resources that each role needs to access for their job function?*
- *Level of privilege required (for example, user, administrator, etc.) for accessing resources?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

7.1.2

Is access to privileged user IDs restricted as follows:

- *To least privileges necessary to perform job responsibilities?*
- *Assigned only to roles that specifically require that privileged access?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

7.1.3 *Is access assigned based on individual personnel's job classification and function?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

7.1.4 *Is documented approval by authorized parties required, specifying required privileges?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

7.2 Is an access control system(s) in place for system components to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed, as follows:

7.2.1 *Is the access control system(s) in place on all system components?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

7.2.2 *Is the access control system(s) configured to enforce privileges assigned to individuals based on job classification and function?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

7.2.3 *Does the access control system(s) have a default "deny-all" setting?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

7.3 *Are security policies and operational procedures for restricting access to cardholder data:*

- *Documented*
- *In use*
- *Known to all affected parties?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Identify and authenticate access to system components

8.1

Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:

8.1.1 *Are all users assigned a unique ID before allowing them to access system components or cardholder data?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.1.2 *Are additions, deletions, and modifications of user IDs, credentials, and other identifier objects controlled such that user IDs are implemented only as authorized (including with specified privileges)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.1.3 *Is access for any terminated users immediately deactivated or removed?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.1.4 *Are inactive user accounts either removed or disabled within 90 days?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.1.5(a) *Are accounts used by third parties to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to users that connect remotely (i.e. from outside your network) to systems that contain cardholder data and only needs to be answered if you allow users to access systems that contain cardholder data remotely. You have indicated in your profile that you do not permit users to access systems that contain cardholder data remotely.

8.1.5(b) *Are third party remote access accounts monitored when in use?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to users that connect remotely (i.e. from outside your network) to systems that contain cardholder data and only needs to be answered if you allow users to access systems that contain cardholder data remotely. You have indicated in your profile that you do not permit users to access systems that contain cardholder data remotely.

8.1.6(a) *Are repeated access attempts limited by locking out the user ID after no more than six attempts?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.1.7 *Once a user account is locked out, is the lockout duration set to a minimum of 30 minutes or until an administrator enables the user ID?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.1.8

If a session has been idle for more than 15 minutes, are users required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session?

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.2 *In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users?*

- *Something you know, such as a password or passphrase*
- *Something you have, such as a token device or smart card*
- *Something you are, such as a biometric*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.2.1(a) *Is strong cryptography used to render all authentication credentials (such as passwords/passphrases) unreadable during transmission and storage on all system components?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.2.2 *Is user identity verified before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.2.3(a) *Are user password parameters configured to require passwords/passphrases meet the following?*

- *A minimum password length of at least seven characters*
- *Contain both numeric and alphabetic characters*

Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.2.4(a) *Are user passwords/passphrases changed at least once every 90 days?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.2.5(a) *Must an individual submit a new password/passphrase that is different from any of the last four passwords/passphrases he or she has used?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

8.2.6 *Are passwords/passphrases set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?*

[X] Yes [ ] No [ ] N/A

8.3 Is all individual non-console administrative access and all remote access to the CDE secured using multi-factor authentication as follows:

Note: *Multi-factor authentication requires that a minimum of two of the three authentication methods (see PCI DSS Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*

8.3.1 *Is multi-factor authentication incorporated for all non-console access into the CDE for personnel with administrative access?*

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. If / when you are compliant with this requirement, please change your answer to yes.

8.3.2 *Is multi-factor authentication incorporated for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to users that connect remotely (i.e. from outside your network) to systems that contain cardholder data and only needs to be answered if you allow users to access systems that contain cardholder data remotely. You have indicated in your profile that you do not permit users to access systems that contain cardholder data remotely.

8.4(a) *Are authentication policies and procedures documented and communicated to all users?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

8.4(b) *Do authentication policies and procedures include the following?*

- *Guidance on selecting strong authentication credentials*
- *Guidance for how users should protect their authentication credentials*
- *Instructions not to reuse previously used passwords*
- *Instructions that users should change passwords if there is any suspicion the password could be compromised*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

8.5 *Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows:*

- *Generic user IDs and accounts are disabled or removed;*
- *Shared user IDs for system administration activities and other critical functions do not exist; and*
- *Shared and generic user IDs are not used to administer any system components?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

8.6 *Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, and certificates, etc.), is the use of these mechanisms assigned as follows?*

- *Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts*
- *Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

8.7 Is all access to any database containing cardholder data (including access by applications, administrators, and all other users) restricted as follows:

8.7(a) *Is all user access to, user queries of, and user actions on (for example, move, copy, delete), the database through programmatic methods only (for example, through stored procedures)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

8.7(b) *Is user direct access to or queries to of databases restricted to database administrators?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

8.7(c) *Are application IDs only able to be used by the applications (and not by individual users or other processes)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

8.8 *Are security policies and operational procedures for identification and authentication:*

- *Documented*
- *In use*
- *Known to all affected parties?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Restrict physical access to cardholder data

9.1 *Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.1.1(a) *Are either video cameras or access-control mechanisms (or both) in place to monitor individual physical access to sensitive areas?*

Note: *"Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present such as the cashier areas in a retail store.*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.1.1(b) *Are either video cameras or access-control mechanisms (or both) protected from tampering or disabling?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.1.1(c) *Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.1.1(d) *Is data collected from video cameras and/or access control mechanisms stored for at least three months unless otherwise restricted by law?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.1.2 *Are physical and/or logical controls in place to restrict access to publicly accessible network jacks?*

For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.1.3 *Is physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines restricted?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any

area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.2(a) *Are procedures developed to easily distinguish between onsite personnel and visitors, which include:*

- *Identifying onsite personnel and visitors (for example, assigning badges),*
- *Changing access requirements, and*
- *Revoking terminated onsite personnel and expired visitor identification (such as ID badges)*

For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.2(b) *Do identification methods (such as ID badges) clearly identify visitors and easily distinguish between onsite personnel and visitors?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.2(c) *Is access to the badge system limited to authorized personnel?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.3 *Is physical access to sensitive areas controlled for onsite personnel, as follows:*

- *Is access authorized and based on individual job function?*
- *Is access revoked immediately upon termination*
- *Upon termination, are all physical access mechanisms, such as keys, access cards, etc., returned or disabled?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.4 Is visitor identification and access handled as follows:

9.4.1 *Are visitors authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained?*

[ ] Compensating Control [ ] Yes [ ] No [X] N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any

area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.4.2(a) *Are visitors identified and given a badge or other identification that visibly distinguishes the visitors from onsite personnel?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.4.2(b) *Do visitor badges or other identification expire?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.4.3 *Are visitors asked to surrender the badge or other identification before leaving the facility or at the date of expiration?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.4.4(a) *Is a visitor log in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.4.4(b) *Does the visitor log contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access?*

☐ Compensating Control ☐ Yes ☐ No ☒ N/A

Not Applicable

Reason not applicable

This question is specific to facilities with sensitive areas and only needs to be answered if you have facilities with sensitive areas. sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes the areas where only point of sale terminals are present, such as the cashier area in a retail store. You have indicated in your profile that you do not have facilities with sensitive areas.

9.4.4(c) *Is the visitor log retained for at least three months?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.5 *Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?*

For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.5.1 *Is the location where media back-ups are stored reviewed at least annually to confirm storage is secure?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

9.6(a) *Is strict control maintained over the internal or external distribution of any kind of media?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.6(b) Do controls include the following:

9.6.1 *Is media classified so the sensitivity of the data can be determined?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.6.2 *Is media sent by secured courier or other delivery method that can be accurately tracked?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.6.3 *Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.7 *Is strict control maintained over the storage and accessibility of media?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.7.1(a) *Are inventory logs of all media properly maintained?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.7.1(b) *Are periodic media inventories conducted at least annually?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

9.8(a) *Is all media destroyed when it is no longer needed for business or legal reasons?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.8(b) *Is there a periodic media destruction policy that defines requirements for the following?*

- *Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.*
- *Storage containers used for materials that are to be destroyed must be secured.*
- *Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.8(c) Is media destruction performed as follows:

9.8.1(a) *Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.8.1(b) *Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.8.2 *Is cardholder data on electronic media rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise by physically destroying the media), so that cardholder data cannot be reconstructed?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.9 Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?

Note: *This requirement applies to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*

9.9(a) *Do policies and procedures require that a list of such devices be maintained?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.9(b) *Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.9(c) *Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

9.9.1(a) *Does the list of devices include the following?*

- *Make, model of device*

- *Location of device (for example, the address of the site or facility where the device is located)*
- *Device serial number or other method of unique identification*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.9.1(b) *Is the list accurate and up to date?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.9.1(c) *Is the list of devices updated when devices are added, relocated, decommissioned, etc.?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.9.2(a) *Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows?*

Note: *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.9.2(b) *Are personnel aware of procedures for inspecting devices?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.9.3

Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?

9.9.3(a) *Do training materials for personnel at point-of-sale locations include the following?*

- *Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.*
- *Do not install, replace, or return devices without verification.*
- *Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).*
- *Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.9.3(b) *Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

9.10 *Are security policies and operational procedures for restricting physical access to cardholder data:*

- *Documented*
- *In use*
- *Known to all affected parties?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Regularly Monitor and Test Networks

Track and monitor all access to network resources and cardholder data

10.1(a) *Are audit trails enabled and active for system components?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.1(b) *Is access to system components linked to individual users?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.2 Are automated audit trails implemented for all system components to reconstruct the following events:

10.2.1 *All individual user accesses to cardholder data?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.2.2 *All actions taken by any individual with root or administrative privileges?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.2.3 *Access to all audit trails?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.2.4 *Invalid logical access attempts?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.2.5 *Use of and changes to identification and authentication mechanisms-including but not limited to creation of new accounts and elevation of privileges - and all changes, additions, or deletions to accounts with root or administrative privileges?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.2.6 *Initialization, stopping, or pausing of the audit logs?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.2.7 *Creation and deletion of system-level objects?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.3 Are the following audit trail entries recorded for all system components for each event:

10.3.1 *User identification?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.3.2 *Type of event?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.3.3 *Date and time?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.3.4 *Success or failure indication?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.3.5 *Origination of event?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.3.6 *Identity or name of affected data, system component, or resource?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.4 *Are all critical system clocks and times synchronized through use of time synchronization technology, and is the technology kept current?*

Note: *One example of time synchronization technology is Network Time Protocol (NTP).*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.4.1 Are the following processes implemented for critical systems to have the correct and consistent time:

10.4.1(a) *Do only designated central time server(s) receive time signals from external sources, and are time signals from external sources based on International Atomic Time or UTC?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.4.1(b) *Where there is more than one designated time server, do the time servers peer with each other to keep accurate time?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.4.1(c) *Do systems receive time only from designated central time server(s)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.4.2

Is time data protected as follows:

10.4.2(a) *Is access to time data restricted to only personnel with a business need to access time data?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.4.2(b) *Are changes to time settings on critical systems logged, monitored, and reviewed?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.4.3 *Are time settings received from specific, industry-accepted time sources? (This is to prevent a malicious individual from changing the clock).*

Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.5

Are audit trails secured so they cannot be altered, as follows:

10.5.1 *Is viewing of audit trails limited to those with a job-related need?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.5.2 *Are audit trail files protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.5.3 *Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.5.4 *Are logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) written onto a secure, centralized, internal log server or media?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.5.5 *Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.6 Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows?

Note: *Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.*

10.6.1(a) *Are written policies and procedures defined for reviewing the following at least daily, either manually or via log tools?*

- *All security events*

- *Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD*
- *Logs of all critical system components*
- *Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.6.1(b) *Are the above logs and security events reviewed at least daily?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.6.2(a) *Are written policies and procedures defined for reviewing logs of all other system components periodically either manually or via log tools based on the organization's policies and risk management strategy?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.6.2(b) *Are reviews of all other system components performed in accordance with organization's policies and risk management strategy?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.6.3(a) *Are written policies and procedures defined for following up on exceptions and anomalies identified during the review process?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.6.3(b) *Is follow up to exceptions and anomalies performed?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

10.7(a) *Are audit log retention policies and procedures in place and do they require that logs are retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.7(b) *Are audit logs retained for at least one year?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.7(c) *Are at least the last three months' logs immediately available for analysis?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

10.9 *Are security policies and operational procedures for monitoring all access to network resources and cardholder data:*

- *Documented*
- *In use*
- *Known to all affected parties?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Regularly test security systems and processes.

11.1(a) *Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis?*

Note: *Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.*

Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

11.1(b) *Does the methodology detect and identify any unauthorized wireless access points, including at least the following?*

- *WLAN cards inserted into system components;*
- *Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and*
- *Wireless devices attached to a network port or network device.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.1(c) *If wireless scanning is utilized to identify authorized and unauthorized wireless access points, is the scan performed at least quarterly for all system components and facilities?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.1(d) *If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), is monitoring configured to generate alerts to notify personnel?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.1.1 *Is an inventory of authorized wireless access points maintained and a business justification documented for all authorized wireless access points?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.1.2(a) *Does the incident response plan define and require a response in the event that an unauthorized wireless access point is detected?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.1.2(b) *Is action taken when unauthorized wireless access points are found?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.2

Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), as follows?

Note: *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.*

For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.

11.2.1(a) *Are quarterly internal vulnerability scans performed?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

11.2.1(b) *Does the quarterly internal scan process address all "high risk" vulnerabilities and include rescans to verify all "high-risk" vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.2.1(c) *Are quarterly internal scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.2.2(a) *Are quarterly external vulnerability scans performed?*

Note: *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).*
Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.2.2(b) *Do external quarterly scan and rescan results satisfy the ASV Program Guide requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.2.2(c) *Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.2.3(a) *Are internal and external scans, and rescans as needed, performed after any significant change?*

Note: *Scans must be performed by qualified personnel.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.2.3(b) *Does the scan process include rescans until:*

- *For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS,*
- *For internal scans, a passing result is obtained or all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.2.3(c) *Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.3 *Does the penetration-testing methodology include the following?*

- *Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)*
- *Includes coverage for the entire CDE perimeter and critical systems*
- *Includes testing from both inside and outside the network*
- *Includes testing to validate any segmentation and scope-reduction controls*
- *Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5*
- *Defines network-layer penetration tests to include components that support network functions as well as operating systems*
- *Includes review and consideration of threats and vulnerabilities experienced in the last 12 months*
- *Specifies retention of penetration testing results and remediation activities results*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.3.1(a) *Is external penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

11.3.1(b) *Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.3.2(a) *Is internal penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

11.3.2(b) *Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.3.3 *Are exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.3.4

If segmentation is used to isolate the CDE from other networks:

11.3.4(a) *Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.3.4(b) *Does penetration testing to verify segmentation controls meet the following?*

- *Performed at least annually and after any changes to segmentation controls /methods*
- *Covers all segmentation controls/methods in use*
- *Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.3.4(c) *Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.4(a) *Are intrusion-detection and/or intrusion-prevention techniques that detect and/or prevent intrusions into the network in place to monitor all traffic:*

- *At the perimeter of the cardholder data environment, and*
- *At critical points in the cardholder data environment.*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.4(b) *Are intrusion-detection and/or intrusion-prevention techniques configured to alert personnel of suspected compromises?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

11.4(c) *Are all intrusion-detection and prevention engines, baselines, and signatures kept up-to-date?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

11.5(a) *Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files?*

Examples of files that should be monitored include:

- *System executables*
- *Application executables*
- *Configuration and parameter files*
- *Centrally stored, historical or archived, log, and audit files*
- *Additional critical files determined by entity (for example, through risk assessment or other means)*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.5(b) *Is the change-detection mechanism configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly?*

Note: *For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.5.1 *Is a process in place to respond to any alerts generated by the change-detection solution?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

11.6 *Are security policies and operational procedures for security monitoring and testing:*

- *Documented*
- *In use*
- *Known to all affected parties?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Maintain an Information Security Policy

Maintain a policy that addresses information security for all personnel.

12.1 *Is a security policy established, published, maintained, and disseminated to all relevant personnel?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.1.1 *Is the security policy reviewed at least annually and updated when the environment changes?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

12.2(a) *Is an annual risk assessment process implemented that*

- *Identifies critical assets, threats, and vulnerabilities, and*
- *Results in a formal, documented analysis of risk?*

Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

12.2(b) *Is the risk assessment process performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.3

Are usage policies for critical technologies developed to define proper use of these technologies and require the following:

Note: *Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.*

12.3.1 *Explicit approval by authorized parties to use the technologies?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.3.2 *Authentication for use of the technology?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.3.3 *A list of all such devices and personnel with access?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.3.4 *A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.3.5 *Acceptable uses of the technologies?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.3.6 *Acceptable network locations for the technologies?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.3.7 *List of company-approved products?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.3.8 *Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.3.9 *Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.3.10(a) *For personnel accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need?*

Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.3.10(b) *For personnel with proper authorization, does the policy require the protection of cardholder data in accordance with PCI DSS Requirements?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.4 *Do security policy and procedures clearly define information security responsibilities for all personnel?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.5(a) *Is responsibility for information security formally assigned to a Chief Security Officer or other security-knowledgeable member of management?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.5(b) Are the following information security management responsibilities formally assigned to an individual or team:

12.5.1 *Establishing, documenting, and distributing security policies and procedures?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.5.2 *Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.5.3 *Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.5.4 *Administering user accounts, including additions, deletions, and modifications?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.5.5 *Monitoring and controlling all access to data?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.6(a) *Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.6(b) Do security awareness program procedures include the following:

12.6.1(a) *Does the security awareness program provide multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions)?*

Note: *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.6.1(b) *Are personnel educated upon hire and at least annually?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

12.6.1(c) *Have employees completed awareness training and are they aware of the importance of cardholder data security?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.6.2 *Are personnel required to acknowledge at least annually that they have read and understood the security policy and procedures?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

12.7 *Are potential personnel (see definition of "personnel" above) screened prior to hire to minimize the risk of attacks from internal sources?*

Examples of background checks include previous employment history, criminal record, credit history and reference checks.

Note: *For those potential personnel to be hired for certain positions, such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.8 Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

12.8.1 *Is a list of service providers maintained, including a description of the service(s) provided?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.8.2 *Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?*

Note: *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.8.3 *Is there an established process for engaging service providers, including proper due diligence prior to engagement?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.8.4 *Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

12.8.5 *Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.10 Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:

12.10.1(a) *Has an incident response plan been created to be implemented in the event of system breach?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.10.1(b)

Does the plan address the following, at a minimum:

12.10.1(b)(i) *Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.10.1(b)(ii) *Specific incident response procedures?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.10.1(b)(iii) *Business recovery and continuity procedures?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.10.1(b)(iv) *Data backup processes?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.10.1(b)(v) *Analysis of legal requirements for reporting compromises?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.10.1(b)(vi) *Coverage and responses of all critical system components?*

[ ] Compensating Control [X] Yes [ ] No [ ] N/A

12.10.1(b)(vii) *Reference or inclusion of incident response procedures from the payment brands?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.10.2 *Is the plan reviewed and tested at least annually, including all elements listed in Requirement 12.10.1?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

Compliance maintenance task

To be compliant this maintenance task must be performed periodically. Please state when it was last performed.

Last Completion Date

08/20/2018

12.10.3 *Are specific personnel designated to be available on a 24/7 basis to respond to alerts?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.10.4 *Is appropriate training provided to staff with security breach response responsibilities?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.10.5 *Are alerts from security monitoring systems included in the incident response plan?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A

12.10.6 *Is a process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?*

☐ Compensating Control ☒ Yes ☐ No ☐ N/A