Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire C-VT

Merchants with Web-Based Virtual Payment Terminals – No Electronic Cardholder Data Storage

For use with PCI DSS Version 3.2
Merchant #: 4223699155229553
Merchant Name: Top Floor Designs

Revision 1.1
January 2017

Section 2: Self-Assessment Questionnaire C-VT

Note: *The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.*

Self-assessment completion date: 10/10/2018

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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?	- Review firewall and router configuration standards - Examine firewall and router configurations	☑	☐	☐	☐
	(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)?	- Review firewall and router configuration standards - Examine firewall and router configurations	☑	☐	☐	☐
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?	- Review firewall and router configuration standards - Examine firewall and router configurations	☑	☐	☐	☐
1.3.4	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	- Examine firewall and router configurations	☑	☐	☐	☐
1.3.5	Are only established connections permitted into the network?	- Examine firewall and router configurations	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	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?	- Review policies and configuration standards - Examine mobile and/or employeeowned devices	☑	☐	☐	☐
	(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?	- Review policies and configuration standards - Examine mobile and/or employeeowned devices	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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, Simple Network Management Protocol (SNMP) community strings, etc.).	- Review policies and procedures - Examine vendor documentation - Observe system configurations and account settings - Interview personnel	☑	☐	☐	☐
	(b) Are unnecessary default accounts removed or disabled before installing a system on the network?	- Review policies and procedures - Review vendor documentation - Examine system configurations and account settings - Interview personnel	☑	☐	☐	☐
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:					
	(a) Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?	- Review policies and procedures - Review vendor documentation - Interview personnel	☑	☐	☐	☐
	(b) Are default SNMP community strings on wireless devices changed at installation?	- Review policies and procedures - Review vendor documentation - Interview personnel - Examine system configurations	☑	☐	☐	☐
	(c) Are default passwords/passphrases on access points changed at installation?	- Review policies and procedures - Interview personnel - Examine system configurations	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(d) Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?	- Review policies and procedures - Interview personnel - Examine system configurations	☑	☐	☐	☐
	(e) Are other security-related wireless vendor defaults changed, if applicable?	- Review policies and procedures - Interview personnel - Examine system configurations	☑	☐	☐	☐
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)?	- Review configuration standards - Examine system configurations	☑	☐	☐	☐
	(b) Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?	- Review configuration standards - Interview personnel - Examine configuration settings - Compare enabled services, etc. to documented justifications	☑	☐	☐	☐
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.	- Review configuration standards - Examine configuration settings	☑	☐	☐	☐
2.2.4	(a) Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?	- Interview personnel	☑	☐	☐	☐
	(b) Are common system security parameters settings included in the system configuration standards?	- Review system configuration standards	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(c) Are security parameter settings set appropriately on system components?	- Examine system components - Examine security parameter settings - Compare settings to system configuration standards	☑	☐	☐	☐
2.2.5	(a) Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	- Examine security parameters on system components	☑	☐	☐	☐
	(b) Are enabled functions documented and do they support secure configuration?	- Review documentation - Examine security parameters on system components	☑	☐	☐	☐
	(c) Is only documented functionality present on system components?	- Review documentation - Examine security parameters on system components	☑	☐	☐	☐
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?	- Examine system components - Examine system configurations - Observe an administrator log on	☑	☐	☐	☐
	(b) Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?	- Examine system components - Examine services and files	☑	☐	☐	☐
	(c) Is administrator access to web-based management interfaces encrypted with strong cryptography?	- Examine system components - Observe an administrator log on	☑	☐	☐	☐
	(d) For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?	- Examine system components - Review vendor documentation - Interview personnel	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
3.2	(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	- Review policies and procedures - Examine system configurations - Examine deletion processes	☑	☐	☐	☐
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?	- Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☑	☐	☐	☐
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	- Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☑	☐	☐	☐
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 the full 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.*	- Review policies and procedures - Review roles that need access to displays of full PAN - Examine system configurations - Observe displays of PAN	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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).	- Review documented standards - Review policies and procedures - Review all locations where CHD is transmitted or received - Examine system configurations	☑	☐	☐	☐
	(b) Are only trusted keys and/or certificates accepted?	- Observe inbound and outbound transmissions - Examine keys and certificates	☑	☐	☐	☐
	(c) Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?	- Examine system configurations	☑	☐	☐	☐
	(d) Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?	- Review vendor documentation - Examine system configurations	☑	☐	☐	☐
	(e For SSL/TLS implementations, is SSL/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. • Cardholder data is only requested if "HTTPS" appears as part of the URL.	- Examine system configurations	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
4.1.1	Are industry best practices (for example, IEEE 802.11i) used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment? Note: The use of WEP as a security control is prohibited.	- Review documented standards - Review wireless networks - Examine system configuration settings	☑	☐	☐	☐
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	- Review policies and procedures	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
5.1	Is anti-virus software deployed on all systems commonly affected by malicious software?	- Examine system configurations	☑	☐	☐	☐
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)?	- Review vendor documentation - Examine system configurations	☑	☐	☐	☐
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?	- Interview personnel	☑	☐	☐	☐
5.2	(a) Are all anti-virus software and definitions kept current?	- Examine policies and procedures - Examine anti-virus configurations, including the master installation - Examine system components	☑	☐	☐	☐
	(b) Are automatic updates and periodic scans enabled and being performed?	- Examine anti-virus configurations, including the master installation - Examine system components	☑	☐	☐	☐
	(c) Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10?	- Examine anti-virus configurations - Review log retention processes	☑	☐	☐	☐
5.3	Are all anti-virus mechanisms: • Actively running? • Unable to be disabled or altered by users?	- Examine anti-virus configurations - Examine system components - Observe processes - Interview personnel	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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?	- Review policies and procedures - Interview personnel - Observe processes	☑	☐	☐	☐
6.2	(a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	- Review policies and procedures	☑	☐	☐	☐
	(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.	- Review policies and procedures - Examine system components - Compare list of security patches installed to recent vendor patch lists	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows: • 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	- Examine written access control policy	☑	☐	☐	☐
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?	- Interview personnel - Interview management - Review privileged user IDs	☑	☐	☐	☐
7.1.3	Are access assigned based on individual personnel's job classification and function?	- Interview management - Review user IDs	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	- Review password procedures - Interview personnel	☑	☐	☐	☐
8.1.3	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)?	- Review password procedures - Examine privileged and general user IDs and associated authorizations - Observe system settings	☑	☐	☐	☐
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	- Review password procedures - Observe authentication processes	☑	☐	☐	☐
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/phrases must have complexity and strength at least equivalent to the parameters specified above.	- Examine system configuration settings to verify password parameters	☑	☐	☐	☐
8.3.1	Is multi-factor authentication incorporated for all nonconsole 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.	- Examine system configurations - Observe administrator logging into CDE	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	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?	- Review policies and procedures - Examine user ID lists - Interview personnel	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	- Observe physical access controls - Observe personnel	☑	☐	☐	☐
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.	- Review policies and procedures for physically securing media - Interview personnel	☑	☐	☐	☐
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	- Review policies and proceduresfor distribution of media	☑	☐	☐	☐
9.6.1	Is media classified so the sensitivity of the data can be determined?	- Review policies and procedures for media classification - Interview security personnel	☑	☐	☐	☐
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	- Interview personnel - Examine media distribution tracking logs and documentation	☑	☐	☐	☐
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	- Interview personnel - Examine media distribution tracking logs and documentation	☑	☐	☐	☐
9.7	Is strict control maintained over the storage and accessibility of media?	- Review policies and procedures	☑	☐	☐	☐
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	- Review periodic media destruction policies and procedures	☑	☐	☐	☐
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	- Interview personnel - Examine procedures - Observe processes	☑	☐	☐	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	- Examine security of storage containers	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Regularly Monitor and Test Networks

Requirement 11: Regularly test security systems and processes

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.3.4	If segmentation is used to isolate the CDE from other networks:					
	(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?	- Examine segementation controls - Review penetration-testing methodology	☑	☐	☐	☐
	(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.	-Examine results from the most recent penetration test	☑	☐	☐	☐
	(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)?	- Interview responsible personnel	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

Note: *For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	- Review the information security policy	☑	☐	☐	☐
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	- Review the information security policy - Interview responsible personnel	☑	☐	☐	☐
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?	- Review usage policies - Interview responsible personnel	☑	☐	☐	☐
12.3.3	A list of all such devices and personnel with access?	- Review usage policies - Interview responsible personnel	☑	☐	☐	☐
12.3.5	Acceptable uses of the technologies?	- Review usage policies - Interview responsible personnel	☑	☐	☐	☐
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	- Review information security policy and procedures - Interview a sample of responsible personnel	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.5	(b) Are the following information security management responsibilities formally assigned to an individual or team:					
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	- Review information security policy and procedures	☑	☐	☐	☐
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	- Review security awareness program	☑	☐	☐	☐
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?	- Review policies and procedures - Observe processes - Review list of service providers	☑	☐	☐	☐
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.	- Observe written agreements - Review policies and procedures	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	- Observe processes - Review policies and procedures and supporting documentation	☑	☐	☐	☐
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	- Observe processes - Review policies and procedures and supporting documentation	☑	☐	☐	☐
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	- Observe processes - Review policies and procedures and supporting documentation	☑	☐	☐	☐
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	- Review the incident response plan - Review incident response plan procedures	☑	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
A2.1	For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS: - Are the devices confirmed to not be susceptible to any known exploits for SSL/early TLS Or: - Is there a formal Risk Mitigation and Migration Plan in place per Requirement A2.2?	- Review documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS	☐	☐	☐	☐
A2.2	Is there a formal Risk Mitigation and Migration Plan in place for all implementations that use SSL and/or early TLS (other than as allowed in A2.1), that includes: - Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; - Risk assessment results and risk reduction controls in place; - Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; - Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; - Overview of migration project plan including target migration completion date no later than 30th June 2018?	- Review the documented Risk Mitigation and Migration Plan	☐	☐	☐	☐

Appendix A3: Designated Entities Supplemental Validation (DESV)

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.

Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example:	
3.4	Cardholder data is never stored electronically

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.