2018 PCI DSS 3.2 Requirements

	REQUIREMENT	GUIDANCE
3.5.1 - Documented Cryptographic Architecture (Service provider requirement)	Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management	Organizations who are subject to PCI DSS compliance should take proactive steps maintain an up to date listing of cryptographic tools being utilized to protect cardholder data.
6.4.6 – Implementation of Requirements (Merchant and service provider requirement)	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	PCI DSS is a rolling and perpetual standard which requires organizations to approach any chances to their environment with compliance considerations in mind. Any significant changes to the PCI CDE (Cardholder Data Environment) may require additional scrutiny on the creation of documentation or reviews of system configurations.
8.3.1 – Multi-factor authentication for non-console access (Merchant and service provider requirement)	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	MFA is a means to confirm a user's claimed identity through knowledge, something they and only they know as well as possession, something they and only they have. MFA creates a defense mechanism which makes it more difficult for hackers or unauthorized users to access system resources.

▷

	REQUIREMENT	GUIDANCE
10.8 – Process for detection and reporting of failures (Service provider requirement)	Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS / IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	Policies and procedures should be reviewed and updated in the event of process changes and should accurately reflect a current state PCI environment. Detection mechanisms should be configured appropriately to alert trained and qualified personnel in the event of critical security control failure.
10.8.1 – Respond to failures of critical security controls (Service provider requirement)	Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	Critical security control failures should be responded to as soon as possible. Any lag time in response or remediation can lead to unauthorized control of system resources, data leakage, or the installation of malicious software. It is necessary that documentation is prepared to support security failure response from an employee and system level perspective.
11.3.4.1 – Confirm PCI DSS Scope (Service provider requirement)	If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls / methods.	Organizations should schedule penetration tests in advance in order to meeting the timing restriction of this requirement. An experience and qualified penetration tester independent of the organizational unit should be consulted to perform this assessment in order to validate confirm the scope of the cardholder data environment.

	REQUIREMENT	GUIDANCE
12.4.1 – Establishing responsibility (Service provider requirement)	Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management	Establishing authority and responsibility for a PCI program within an organizational is an essential step in maintaining compliance. Aligning strategy with explicit requirements allows for increased level of cybersecurity and protection of sensitive customer data. Executive management's role in PCI compliance promotes a more holistic approach to data security.
12.11 – Perform quarterly reviews (Service provider requirement)	Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	Quarterly reviews of PCI procedures help to promote accountability within and organization. Dedicating time and resources to maintaining PCI compliance. It is essential to document the results of all quarterly reviews and train employees to be familiar with the specific PCI requirements aforementioned.
12.11.1 – Maintain documentation of quarterly review process (Service provider requirement)	Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	Quarterly reviews allow organizations to keep a pulse on their PCI DSS program. Retaining appropriate documentation and evidence of quarterly reviews helps to support the completion of required PCI DSS procedures.

CLICK HERE
to contact us and learn more.

Trust earned.

FreedMaxick®