

ISO 27001 Title	Number	PCI DSS 2.0 Requirement
4 Information security management system		
4.1 General requirements		
4.2 Establishing and managing the ISMS		
4.2.1 Establish the ISMS		
4.2.1.a		
4.2.1.b		
4.2.1.b.1		
4.2.1.b.2		
4.2.1.b.3		
4.2.1.b.4		
4.2.1.b.5		
4.2.1.c	12.1.2	Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.
4.2.1.c.1		
4.2.1.c.2		
4.2.1.d		
4.2.1.d.1		
4.2.1.d.2		
4.2.1.d.3		
4.2.1.d.4		
4.2.1.e		
4.2.1.e.1		
4.2.1.e.2		
4.2.1.e.3		
4.2.1.e.4		
4.2.1.f		
4.2.1.f.1		
4.2.1.f.2		
4.2.1.f.3		
4.2.1.f.4		
4.2.1.g		
4.2.1.h		
4.2.1.i		
4.2.1.j		
4.2.1.j.1		
4.2.1.j.2		
4.2.1.j.3		
4.2.2 Implement and operate the ISMS		
4.2.2.a		
4.2.2.b		
4.2.2.c		
4.2.2.d		
4.2.2.e		
4.2.2.f		
4.2.2.g		
4.2.2.h		
4.2.3 Monitor and review the ISMS		
4.2.3 a		
4.2.3.a.1		
4.2.3.a.2		
4.2.3.a.3		
4.2.3.a.4		
4.2.3.a.5		

5.2.1.c		
5.2.1.d		
5.2.1.e		
5.2.1.f		
5.2.2 Training, awareness and competence		
5.2.2.a		
5.2.2.b		
5.2.2.c		
5.2.2.d		
6 Internal ISMS audits		
6.a		
6.b		
6.c		
6.d		
7 Management review of the ISMS		
7.1 General		
7.2 Review input		
7.2.a		
7.2.b		
7.2.c		
7.2.d		
7.2.e		
7.2.f		
7.2.g		
7.2.h		
7.2.i		
7.3 Review output		
7.3.a		
7.3.b		
7.3.c		
7.3.c.1		
7.3.c.2		
7.3.c.3		
7.3.c.4		
7.3.c.5		
7.3.c.6		
7.3.d		
7.3.e		
8 ISMS improvement		
8.1 Continual improvement		
8.2 Corrective action		
8.2.a		
8.2.b		
8.2.c		
8.2.d		
8.2.e		
8.2.f		
8.3 Preventive action		
8.3.a		

8.3.b		
8.3.c		
8.3.d		
8.3.e		
Appendix A		
A.5 Security Policy		
A.5.1 Information Security Policy		
A.5.1.1 Information Security Policy Document	12.1	Establish, publish, maintain, and disseminate a security policy that accomplishes the following:
A.5.1.2 Review of the information security policy	12.1.3	Includes a review at least annually and updates when the environment changes.
A.6 Organization of Information Security		
A.6.1 Internal Organization		
A.6.1.1 Management Commitment to information security		
A.6.1.2 Information security coordination		
A.6.1.3 Allocation of information security responsibilities	12.5	Assign to an individual or team the following information security management responsibilities:
	12.5.1	Establish, document, and distribute security policies and procedures.
	12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.
	12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
	12.5.4	Administer user accounts, including additions, deletions, and modifications
	12.5.5	Monitor and control all access to data.
A.6.1.4 Authorization process for information processing facilities		
A.6.1.5 Confidentiality agreements		
A.6.1.6 Contact with authorities		
A.6.1.7 Contact with special interest groups		
A.6.1.8 Independent review of information security		
A.6.2 External Parties		
A.6.2.1 Identification of risks related to external parties		
A.6.2.2 Addressing security when dealing with customers		
A.6.2.3 Addressing security in third party agreements	12.8	If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:
	12.8.1	Maintain a list of service providers.
	12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.
	12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
A.7 Asset Management		
A.7.1 Responsibility for assets		
A.7.1.1 Inventory of assets	12.3.3	A list of all such devices and personnel with access
A.7.1.2 Ownership of assets	12.3.4	Labeling of devices to determine owner, contact information and purpose
A.7.1.3 Acceptable use of assets	12.3	Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:
	12.3.1	Explicit approval by authorized parties
	12.3.5	Acceptable uses of the technology
	12.3.6	Acceptable network locations for the technologies
	12.3.7	List of company-approved products
A.7.2 Information classification		
A.7.2.1 Classification guidelines	9.7.1	Classify media so the sensitivity of the data can be determined.
A.7.2.2 Information labelling and handling		
A.8 Human resources security		
A.8.1 Prior to employment		
A.8.1.1 Roles and responsibilities	12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

A.8.1.2 Screening	12.7	Screen potential personnel 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.)
A.8.1.3 Terms and conditions of employment		
A.8.2 During employment		
A 8.2.1 Management responsibilities		
A 8.2.2 Information security awareness, education and training	12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
	12.6.1	Educate personnel upon hire and at least annually.
	12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.
	12.9.4	Provide appropriate training to staff with security breach response responsibilities.
A 8.2.3 Disciplinary process		
A.8.3 Termination or change of employment		
A 8.3.1 Termination responsibilities		
A 8.3.2 Return of assets		
A 8.3.3 Removal of access rights	8.5.4	Immediately revoke access for any terminated users.
A.9 Physical and environmental security		
A.9.1 Secure Areas		
A 9.1.1 Physical security perimeter		
A 9.1.2 Physical entry controls	9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
	9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.
	9.2	Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.
	9.3	Make sure all visitors are handled as follows:
	9.3.1	Authorized before entering areas where cardholder data is processed or maintained.
	9.3.2	Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.
	9.3.3	Asked to surrender the physical token before leaving the facility or at the date of expiration.
	9.4	Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.
A 9.1.3 Securing offices, rooms and facilities		
A 9.1.4 Protecting against external and environmental threats		
A 9.1.5 Working in secure areas		
A 9.1.6 Public access, delivery and loading areas		
A.9.2 Equipment Security		
A 9.2.1 Equipment siting and protection	9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.
A 9.2.2 Supporting utilities		
A 9.2.3 Cabling security	9.1.2	Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.
A 9.2.4 Equipment maintenance		
A 9.2.5 Security of equipment off-premises		
A 9.2.6 Secure disposal or re-use of equipment		
A 9.2.7 Removal of property		
A.10 Communications and operations management		
A.10.1 Operational procedures and responsibilities		
A 10.1.1 Documented operating procedures	12.2	Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).
A 10.1.2 Change management	1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations
	6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:
	6.4.5	Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:
	6.4.5.1	Documentation of impact.
	6.4.5.2	Documented change approval by authorized parties.

	6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.
	6.4.5.4	Back-out procedures.
A 10.1.3 Segregation of duties	6.4.2	Separation of duties between development/test and production environments
A 10.1.4 Separation of development, test and operational facilities	6.4.1	Separate development/test and production environments
A.10.2 Third party service delivery management		
A 10.2.1 Service delivery		
A 10.2.2 Monitoring and review of third party services	12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
A 10.2.3 Managing changes to third party services		
A.10.3 System planning and acceptance		
A 10.3.1 Capacity Management		
A 10.3.2 System acceptance		
A.10.4 Protection against malicious and mobile code		
A 10.4.1 Controls against malicious code	5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
	5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
	5.2	Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
A 10.4.2 Controls against mobile code		
A.10.5 BackUp		
A 10.5.1 Information Backup	9.5	Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.
A 10.6 Network security management		
A 10.6.1 Network controls	1.1	Establish firewall and router configuration standards that include the following
	1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks.
	1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.
	1.1.6	Requirement to review firewall and router rule sets at least every six months
	1.2.2	Secure and synchronize router configuration files.
	2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
	4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
	11.4	Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.
	11.4	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.
	2.2.2	Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.
	6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes - Installing a web-application firewall in front of public-facing web applications
A 10.6.2 Security of network services		
A.10.7 Media Handling		
A 10.7.1 Management of removable media		
A 10.7.2 Disposal of media	9.10	Destroy media when it is no longer needed for business or legal reasons as follows: Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
	9.10.1	
A 10.7.3 Information handling procedures	9.6	Physically secure all media.
	9.7	Maintain strict control over the internal or external distribution of any kind of media, including the following:
	9.8	Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).
	9.9	Maintain strict control over the storage and accessibility of media.

	9.9.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.
	12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.
	3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.
	3.1.1	Implement a data retention and disposal policy that includes: - Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements - Processes for secure deletion of data when no longer needed - Specific retention requirements for cardholder data - A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements
	3.2	Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.
	3.2.1	Do not store 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). 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 - Service code To minimize risk, store only these data elements as needed for business.
	3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.
	3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.
	3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Notes: - This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN. - This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.
	3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in 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) <input type="checkbox"/> Strong cryptography with associated key-management processes and procedures
	3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.
	9.10.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
A 10.7.4 Security of system documentation		
A.10.8 Exchange of information		
A 10.8.1 Information exchange policies and procedures		
A 10.8.2 Exchange agreements		
A 10.8.3 Physical media in transit		
	9.7.2	Send the media by secured courier or other delivery method that can be accurately tracked.
A 10.8.4 Electronic messaging		
	10.8.4	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).
A 10.8.5 Business information systems		
A.10.9 Electronic commerce services		
A 10.9.1 Electronic commerce		
A 10.9.2 On-line transactions		
A 10.9.3 Publicly available information		
A.10.10 Monitoring		
A 10.10.1 Audit logging		
	A.1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.
	10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
	10.2	Implement automated audit trails for all system components to reconstruct the following events:
	10.2.1	All individual accesses to cardholder data
	10.2.2	All actions taken by any individual with root or administrative privileges
	10.2.3	Access to all audit trails
	10.2.4	Invalid logical access attempts
	10.2.5	Use of identification and authentication mechanisms
	10.2.6	Initialization of the audit logs
	10.2.7	Creation and deletion of system-level objects
	10.3	Record at least the following audit trail entries for all system components for each event:

	10.3.1	User identification
	10.3.2	Type of event
	10.3.3	Date and time
	10.3.4	Success or failure indication
	10.3.5	Origination of event
	10.3.6	Identity or name of affected data, system component, or resource.
	10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).
A 10.10.2 Monitoring system use	10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).
A 10.10.3 Protection of log information	10.5	Secure audit trails so they cannot be altered.
	10.5.1	Limit viewing of audit trails to those with a job-related need.
	10.5.2	Protect audit trail files from unauthorized modifications.
	10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
	10.5.4	Write logs for external-facing technologies onto a log server on the internal LAN.
	10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
A 10.10.4 Administrator and operator logs		
A 10.10.5 Fault logging		
A 10.10.6 Clock synchronization	10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.
	10.4.1	Critical systems have the correct and consistent time.
	10.4.2	Time data is protected.
	10.4.3	Time settings are received from industry-accepted time sources.
A.11 Access control		
A.11.1 Business requirement for access control		
A 11.1.1 Access control policy	2.1	Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
	7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:
	7.1.4	Implementation of an automated access control system
	7.2	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:
	7.2.1	Coverage of all system components
	7.2.2	Assignment of privileges to individuals based on job classification and function
	7.2.3	Default "deny-all" setting
	8.2	In addition to assigning a unique ID, employ at least one of the following methods 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
	8.5	Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:
	8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
	8.5.10	Require a minimum password length of at least seven characters.
	8.5.11	Use passwords containing both numeric and alphabetic characters.
A.11.2 User access management		
A 11.2.1 User registration	7.1.3	Requirement for a documented approval by authorized parties specifying required privileges.
A 11.2.2 Privilege management	7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities
	7.1.2	Assignment of privileges is based on individual personnel's job classification and function
A 11.2.3 User password management	8.5.2	Verify user identity before performing password resets
	8.5.3	Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.
	8.5.7	Communicate authentication procedures and policies to all users who have access to cardholder data.
	8.5.9	Change user passwords at least every 90 days.
A 11.2.4 Review of user access rights	8.5.5	Remove/disable inactive user accounts at least every 90 days.
A.11.3 User responsibilities		
A 11.3.1 Password use		
A 11.3.2 Unattended user equipment		
A 11.3.3 Clear desk and clear screen policy		
A.11.4 Network access control		
A 11.4.1 Policy on use of network services	1.1.4	Description of groups, roles, and responsibilities for logical management of network components
	8.3	Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)
A 11.4.2 User authentication for external connections	8.3	Enable accounts used by vendors for remote access only during the time period needed.
	8.5.6	Monitor vendor remote access accounts when in use.

	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
A 11.4.3 Equipment identification in networks		
A 11.4.4 Remote diagnostic and configuration port protection		
A 11.4.5 Segregation in networks	1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
	1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. 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	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
	1.2.3	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
	1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.
	1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
	1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.
	1.3.3	Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.
	1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ.
	1.3.5	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
	1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)
	1.3.7	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
	1.3.8	Do not disclose private IP addresses and routing information to unauthorized parties.
A 11.4.6 Network connection control		
A 11.4.7 Network routing control		
A.11.5 Operating system access control		
A 11.5.1 Secure log-on procedures	8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.
	8.5.14	Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
A 11.5.2 User identification and authentication	8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.
	8.5.8	Do not use group, shared, or generic accounts and passwords, or other authentication methods.
	12.3.2	Authentication for use of the technology
A 11.5.3 Password management system	8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
A 11.5.4 Use of system utilities		
A 11.5.5 Session time-out	8.5.15	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
	12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
A 11.5.6 Limitation of connection time		
A.11.6 Application and information access control		
A 11.6.1 Information access restriction	8.5.16	Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.
A 11.6.2 Sensitive system isolation	2.2.1	Implement only one primary function 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.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.
	2.4	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.
	A.1	Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.
	A.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.
	A.1.2	Restrict each entity's access and privileges to its own cardholder data environment only.
A.11.7 Mobile computing and teleworking		
A 11.7.1 Mobile computing and communications		
A 11.7.2 Teleworking		
A.12 Information systems acquisition, development and maintenance		

A.12.1 Security requirements of information systems		
A 12.1.1 Security requirements analysis and specification	6.3	Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:
	6.3.2	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.
A.12.2 Correct processing in applications	6.5	Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:
	6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.
	6.5.2	Buffer overflow
	6.5.3	Insecure cryptographic storage
	6.5.4	Insecure communications
	6.5.5	Improper error handling
	6.5.6	All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).
	6.5.7	Cross-site scripting (XSS)
	6.5.8	Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)
	6.5.9	Cross-site request forgery (CSRF)
A 12.2.1 Input data validation		
A 12.2.2 Control of internal processing		
A 12.2.3 Message integrity		
A 12.2.4 Output data validation		
A.12.3 Cryptographic controls		
A 12.3.1 Policy on the use of cryptographic controls	8.4	Render all passwords unreadable during transmission and storage on all system components using strong cryptography.
	2.3	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.
	4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.
A 12.3.2 Key management	3.5	Protect any keys used to secure cardholder data against disclosure and misuse:
	3.5.1	Restrict access to cryptographic keys to the fewest number of custodians necessary.
	3.5.2	Store cryptographic keys securely in the fewest possible locations and forms.
	3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:
	3.6.1	Generation of strong cryptographic keys
	3.6.2	Secure cryptographic key distribution
	3.6.3	Secure cryptographic key storage
	3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of ciphertext 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).
	3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised.
	3.6.6	If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).
	3.6.7	Prevention of unauthorized substitution of cryptographic keys.
	3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.
A.12.4 Security of system files	2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: - Center for Internet Security (CIS) - International Organization for Standardization (ISO) - SysAdmin Audit Network Security (SANS) Institute - National Institute of Standards Technology (NIST)
	11.5	Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
A 12.4.1 Control of operational software	2.2.3	Configure system security parameters to prevent misuse.
	2.2.4	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
	6.3.1	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers
	6.4.4	Removal of test data and accounts before production systems become active
A 12.4.2 Protection of system test data	6.4.3	Production data (live PANs) are not used for testing or development
A 12.4.3 Access control to program source code		
A.12.5 Security in development and support processes		
A 12.5.1 Change control procedures		

A 12.5.2 Technical review of applications after operating system changes		
A 12.5.3 Restrictions on changes to software packages		
A 12.5.4 Information leakage		
A 12.5.5 Outsourced software development		
A.12.6 Technical Vulnerability Management		
A 12.6.1 Control of Technical Vulnerabilities	6.1	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.
	6.2	Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.
	11.1	Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.
	11.2	Run internal and external network vulnerability scans 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).
	11.2.1	Perform quarterly internal vulnerability scans.
	11.2.2	Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).
	11.2.3	Perform internal and external scans after any significant change.
	11.3	Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:
	11.3.1	Network-layer penetration tests
	11.3.2	Application-layer penetration tests
A.13 Information security incident management		
A.13.1 Reporting information security events and weaknesses		
A 13.1.1 Reporting information security events		
A 13.1.2 Reporting security weaknesses		
A.13.2 Management of information security incidents and improvements		
A 13.2.1 Responsibilities and procedures	12.9	Implement an incident response plan. Be prepared to respond immediately to a system breach.
	12.9.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: - Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business recovery and continuity procedures - Data back-up processes - Analysis of legal requirements for reporting compromises - Coverage and responses of all critical system components - Reference or inclusion of incident response procedures from the payment brands
	12.9.2	Test the plan at least annually.
	12.9.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.
	12.9.5	Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.
A 13.2.2 Learning from information security incidents	12.9.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
A 13.2.3 Collection of evidence	A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.
A.14 Business continuity management		
A.14.1 Information Security Aspects of business continuity management		
A 14.1.1 Including information security in the business continuity management process		
A 14.1.2 Business continuity and risk assessment		
A 14.1.3 Development and implementing continuity plans including information security		
A 14.1.4 Business Continuity planning framework		
A 14.1.5 Testing, maintaining and reassessing business continuity plans		
A.15 Compliance		
A.15.1 Compliance with legal requirements		
A 15.1.1 Identification of applicable legislation		

A 15.1.2 Intellectual property rights (IPR)		
A 15.1.3 Protection of organizational records		
A 15.1.4 Data protection and privacy of personal information		
A 15.1.5 Prevention of misuse of information processing facilities		
A 15.1.6 Regulation of cryptographic controls		
A.15.2 Compliance with security policies and standards and technical compliance		
A 15.2.1 Compliance with security policies and standards	12.1.1	Addresses all PCI DSS requirements.
A 15.2.2 Technical compliance checking		
A.15.3 Information systems audit considerations		
A 15.3.1 Information systems audit controls		
A 15.3.2 Protection of information systems audit tools		