

Mapping ISO 27001 Controls to PCI-DSS V1.2 Requirements



This work is copyright © 2009, [Mohan Kamat](#) and [ISO27k implementers' forum](#), some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.).

PCI-DSS V1.2 Requirement		ISO 27001 Control	
Build & Maintain Secure Network			
Requirement 1 – Install & Maintain Firewall Configuration to maintain data			
1.1	Establish firewall and router configuration standards that include the following	A.10.6.1	Network Controls
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	A.10.1.2	Change Management
1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	A.10.6	Network Security Management
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	A.11.4.5	Segregation in networks
1.1.4	Description of groups, roles, and responsibilities for logical management of network components	A.11.4.1	Policy on use of network services
		A.11.4.7	Network routing control
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	A.10.1.1	Documented operating procedures
1.1.6	Requirement to review firewall and router rule sets at least every six months	A.10.6	Network Security Management
1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	A.11.4.5	Segregation in networks
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment	A.11.4.5	Segregation in networks
1.2.2	Secure & synchronise router configuration files	A.10.6	Network Security Management
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.	A.11.4.5	Segregation in networks
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 and outbound traffic to only protocols that are necessary for the cardholder data environment.	A.11.4.5	Segregation in networks

PCI-DSS V1.2 Requirement		ISO 27001 Control	
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	A.11.4.5	Segregation in networks
1.3.3	Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	A.11.4.5	Segregation in networks
1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ.	A.11.4.5	Segregation in networks
1.3.5	Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	A.11.4.5	Segregation in networks
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	A.11.4.6	Network Connection Control
1.3.7	Place the database in an internal network zone, segregated from the DMZ.	A.11.4.5	Segregation in networks
1.3.8	Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).	A.11.4.5	Segregation in networks
1.4	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.	A.11.4.6	Network Connection Control
Requirement 2 - Do not use vendor supplied defaults for systems, passwords and other security parameters			
2.1	Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	A.11.1.1	Access Control Policy
		A.11.2.3	User password management
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. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	A.10.6.1	Network Controls
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	A.12.4	Security of SystemFiles

PCI-DSS V1.2 Requirement		ISO 27001 Control	
2.2.1	Implement only one primary function per server.	A.11.6.2	Sensitive system isolation
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).	A.10.6.2	Security of network services
2.2.3	Configure system security parameters to prevent misuse.	A.10.6.2	Security of network services
2.2.4	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	A.12.4.1	Control of operational software
		A.11.4.4	Remote diagnostic and configuration port protection
		A.11.5.4	Use of system utilities
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for webbased management and other non-console administrative access.	A.11.5.1	Secure log-on procedures
		A.11.5.2	User identification and authentication
		A.11.4.4	Remote diagnostic and configuration port protection
		A.10.6.1	Network Controls
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.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment	A.11.4.5	Segregation in networks
A.1.2	Restrict each entity's access and privileges to own cardholder data environment only.	A.11.4.5	Segregation in networks
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.	A.10.10.1	Audit Logging
A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any provider.	A.10.10.1	Audit Logging
Protect Cardholder Data			
Requirement 3 - Protect stored cardholder data			
3.1	Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention	A.15.13	Protection of organizational records

PCI-DSS V1.2 Requirement		ISO 27001 Control	
	time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.		
3.2	Do not store sensitive authentication data after authorization (even if encrypted).		
3.2.1	Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	A.15.2.1	Compliance with security policies and standards
3.2.2	Do not store the card verification code or value (threedigit or four-digit number printed on the front or back of a payment card) used to verify card-not present transactions.	A.15.2.1	Compliance with security policies and standards
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	A.15.2.1	Compliance with security policies and standards
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)	A.15.2.1	Compliance with security policies and standards
3.4	Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs)	A.12.3.1	Policy on the use of cryptographic controls
		A.10.6.2	Security of network services
		A.10.7.2	Disposal of media
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	A.10.6.2	Security of network services
		A.10.7.2	Disposal of media
3.5	Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse	A.12.3.2	Key management
3.5.1	Restrict access to cryptographic keys to the fewest number of custodians necessary.	A.12.3.2	Key management
3.5.2	Store cryptographic keys securely in the fewest possible locations and forms.	A.12.3.2	Key management
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data	A.12.3.2	Key management
		A.10.1.2	Change Management
		A.12.5.1	Change control procedure
3.6.1	Generation of strong cryptographic keys	A.12.3.2	Key management

PCI-DSS V1.2 Requirement		ISO 27001 Control	
3.6.2	Secure cryptographic key distribution	A.12.3.2	Key management
3.6.3	Secure cryptographic key storage	A.12.3.2	Key management
3.6.4	Periodic cryptographic key changes	A.10.1.2	Change Management
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys	A.12.3.2	Key management
3.6.6	Split knowledge and establishment of dual control of cryptographic keys	A.12.3.2	Key management
3.6.7	Prevention of unauthorized substitution of cryptographic keys	A.12.3.2	Key management
3.6.8	Requirement for cryptographic key custodians to sign a form stating that they understand and accept their keycustodian responsibilities	A.12.3.2	Key management
Requirement 4 - Encrypt transmission of cardholder data across open, public networks			
4.1	Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.	A.10.6.1	Network Controls
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices	A.10.6.1	Network Controls
		A.10.8.1	Information exchange policies and procedures
		A.11.4.2	User authentication for external connections
4.2	Never send unencrypted PANs by end-user messaging technologies	A.10.8.4	Electronic messaging
Maintain a Vulnerability Management Program			
Requirement 5 - Vulnerability Management Program			
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	A.10.4	Protection against malicious and mobile code
5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	A.10.4	Protection against malicious and mobile code
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	A.10.4	Protection against malicious and mobile code
Requirement 6 – Develop and maintain secure systems and applications			

PCI-DSS V1.2 Requirement		ISO 27001 Control	
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	A.6.1.7	Contact with special interest groups
		A.12.4.1	Control of operational software
		A.12.5.1	Change control procedure
		A.12.6.1	Control of technical vulnerabilities
6.2	Establish a process to identify newly discovered security vulnerabilities	A.12.6.1	Control of technical vulnerabilities
6.3	Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:	A.12.1.1	Security requirements analysis and specification
		A.12.2.1	Input data validation
		A.12.2.2	Control of internal processing
		A.12.5.2	Technical review of applications after operating system changes
6.3.1	Testing of all security patches, and system and software configuration changes before deployment, including but not limited to the following:	A.10.1.2	Change Management
6.3.1.1	Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	A.12.2.1	Input data validation
6.3.1.2	Validation of proper error handling	A.10.10.5	Fault logging
6.3.1.3	Validation of secure cryptographic storage	A.12.3.2	Key management
6.3.1.4	Validation of secure communications	A.12.3.1	Policy on use of cryptographic controls
		A.11.4	Network Access control
6.3.1.5	Validation of proper rolebased access control (RBAC)	A.11.1.1	Access Control Policy
6.3.2	Separate development/test and production environments	A.10.1.4	Separation of development, test and operational facilities
6.3.3	Separation of duties between development/test and production environments	A.10.1.3	Segregation of duties
6.3.4	Production data (live PANs) are not used for testing or development	A.10.1.2	Change Management

PCI-DSS V1.2 Requirement		ISO 27001 Control	
6.3.5	Removal of test data and accounts before production systems become active	A.10.1.4	Separation of development, test and operational facilities
6.3.6	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	A.11.1.1	Access Control Policy
		A.11.2.3	User password management
6.3.7	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability	A.12.5.2	Technical review of applications after operating system changes
6.4	Follow change control procedures for all changes to system components. The procedures must include the following:	A.10.1.2	Change Management
6.4.1	Documentation of impact	A.10.1.2	Change Management
6.4.2	Management sign-off by appropriate parties	A.10.1.2	Change Management
6.4.3	Testing of operational functionality	A.10.1.2	Change Management
6.4.4	Back-out procedures	A.10.1.2	Change Management
6.5	Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the OWASP Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following:	A.12.1.1	Security requirements analysis and specification
6.5.1	Cross-site scripting (XSS)	A.12.1.1	Security requirements analysis and specification
6.5.2	Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.	A.12.1.1	Security requirements analysis and specification
6.5.3	Malicious file execution	A.10.4.1	Controls against malicious code
6.5.4	Insecure direct object references	A.12.1.1	Security requirements analysis and specification
6.5.5	Cross-site request forgery (CSRF)	A.12.1.1	Security requirements analysis and specification
6.5.6	Information leakage and improper error handling	A.10.10.5	Fault logging
		A.12.5.4	Information Leakage
6.5.7	Broken authentication and session management	A.11.4.2	User authentication for external connections

PCI-DSS V1.2 Requirement		ISO 27001 Control	
6.5.8	Insecure cryptographic storage	A.12.3.1	Policy on the use of cryptographic controls
6.5.9	Insecure communications	A.11.4.1	Policy on use of network services
6.5.10	Failure to restrict URL access	A.11.4	Network Access control
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	A.12.6.1	Control of technical vulnerabilities
Implement Strong Access Control Measures			
Requirement 7 - Restrict access to cardholder data by business need to know			
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:	A.11.1.1	Business requirement for access control
		A.11.2	User Access Management
7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	A.11.2.2	Privilege Management
7.1.2	Assignment of privileges is based on individual personnel's job classification and function	A.11.2.2	Privilege Management
7.1.3	Requirement for an authorization form signed by management that specifies required privileges	A.11.2.1	User Registration
7.1.4	Implementation of an automated access control system	A.11.1.1	Access Control Policy
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 following	A.11.2	User Access Management
7.2.1	Coverage of all system components	A.11.1.1	Access Control Policy
7.2.2	Assignment of privileges to individuals based on job classification and function	A.11.2.2	Privilege Management
7.2.3	Default "deny-all" setting	A.11.1.1	Access Control Policy
Requirement 8 - Assign an unique ID to each person with computer access			
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	A.11.2.1	User Registration
8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: Password or passphrase	A.11.1.1	Access Control Policy

PCI-DSS V1.2 Requirement		ISO 27001 Control	
	and Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)		
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.	A.11.1.1	Access Control Policy
		A.11.4.1	Policy on use of network services
8.4	Render all passwords unreadable during transmission and storage on all system components using strong cryptography	A.11.2.3	User password management
8.5	Ensure proper user authentication and password management for nonconsumer users and administrators on all system components as follows:	A.11.2	User Access Management
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	A.11.1.1	Access Control Policy
8.5.2	Verify user identity before performing password resets	A.11.2.3	User password management
8.5.3	Set first-time passwords to a unique value for each user and change immediately after the first use.	A.11.2.3	User password management
8.5.4	Immediately revoke access for any terminated users.	A.8.3.3	Removal of access rights
8.5.5	Remove/disable inactive user accounts at least every 90 days.	A.11.2.4	Review of user access rights
8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed.	A.11.4.6	Network Connection Control
8.5.7	Communicate password procedures and policies to all users who have access to cardholder data.	A.11.2.3	User password management
8.5.8	Do not use group, shared, or generic accounts and passwords.	A.11.5.2	User identification and authentication
8.5.9	Change user passwords at least every 90 days.	A.11.5.3	Password management system
8.5.10	Require a minimum password length of at least seven characters.	A.11.3.1	Password Use
8.5.11	Use passwords containing both numeric and alphabetic characters.	A.11.3.1	Password Use
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.11.5.3	Password management system
8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.	A.11.5.1	Secure log-on procedures
8.5.14	Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	A.11.5.5	Session time out

PCI-DSS V1.2 Requirement		ISO 27001 Control	
8.5.15	If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.	A.11.5.5	Session time out
		A.11.3.3	Clear desk and clear screen policy
8.5.16	Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.	A.11.6	Application and information access control
		A.10.10.1	Audit Logging
Requirement 9 - Restrict Physical Access to card holder data			
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	A.9.1.1	Physical security perimeter
9.1.1	Use video cameras or other 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.	A.9.1.2	Physical entry controls
9.1.2	Restrict physical access to publicly accessible network jacks.	A.9.2.3	Cabling Security
9.1.3	Restrict physical access to wireless access points, gateways, and handheld devices.	A.9.2.1	Equipment siting and protection
9.2	Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.	A.9.1.2	Physical entry controls
9.3	Make sure all visitors are handled as follows:	A.9.1.2	Physical entry controls
9.3.1	Authorized before entering areas where cardholder data is processed or maintained	A.9.1.2	Physical entry controls
9.3.2	Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees	A.9.1.3	Securing offices, rooms, and facilities
9.3.3	Asked to surrender the physical token before leaving the facility or at the date of expiration	A.9.1.2	Physical entry controls
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 employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law	A.9.1.2	Physical entry controls
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.9.1.4	Protecting against external and environmental threats
		A.10.5.1	Information Backup

PCI-DSS V1.2 Requirement		ISO 27001 Control	
		A.10.7.1	Management of removable media
9.6	Physically secure all paper and electronic media that contain cardholder data	A.9.1.4	Protecting against external and environmental threats
		A.10.7.1	Management of removable media
9.7	Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data, including the following:	A.10.8.1	Information exchange policies and procedures
		A.10.7.1	Management of removable media
9.7.1	Classify the media so it can be identified as confidential	A.7.2.2	Information labeling and handling
		A.10.7.3	Information handling procedures
9.7.2	Send the media by secured courier or other delivery method that can be accurately tracked.	A.10.8.3	Physical media in transit
9.8	Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals)	A.8.1.3	Terms and conditions of employment
		A.10.1.1	Documented operating procedures
		A.10.7.1	Management of removable media
9.9	Maintain strict control over the storage and accessibility of media that contains cardholder data.	A.10.7.1	Management of removable media
9.9.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	A.10.7.1	Management of removable media
9.10	Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows	A.10.7.2	Disposal of media
9.10.1	Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	A.10.7.2	Disposal of media
9.10.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	A.10.7.2	Disposal of media
Regularly monitor & test networks			
Requirement 10 - Track & monitor all access to network resources & cardholder data			
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.	A.10.10.1	Audit Logging
10.2	Implement automated audit trails for all system components to	A.10.10.1	Audit Logging

PCI-DSS V1.2 Requirement		ISO 27001 Control	
	reconstruct the following events:		
10.2.1	All individual accesses to cardholder data	A.10.10.1	Audit Logging
10.2.2	All actions taken by any individual with root or administrative privileges	A.10.10.1	Audit Logging
10.2.3	Access to all audit trails	A.10.10.3	Protection of log information
10.2.4	Invalid logical access attempts	A.10.10.2	Monitoring system use
10.2.5	Use of identification and authentication mechanisms	A.11.5.1	Secure log-on procedures
10.2.6	Initialization of the audit logs	A.10.10.3	Protection of log information
10.2.7	Creation and deletion of system-level objects	A.10.10.1	Audit Logging
10.3	Record at least the following audit trail entries for all system components for each event:	A.10.10.1	Audit Logging
10.3.1	User identification	A.10.10.1	Audit Logging
10.3.2	Type of event	A.10.10.1	Audit Logging
10.3.3	Date and time	A.10.10.1	Audit Logging
10.3.4	Success or failure indication	A.10.10.1	Audit Logging
10.3.5	Origination of event	A.10.10.1	Audit Logging
10.3.6	Identity or name of affected data, system component, or resource	A.10.10.1	Audit Logging
10.4	Synchronize all critical system clocks and times.	A.10.10.6	Clock Synchronisation
10.5	Secure audit trails so they cannot be altered.	A.10.10.2	Monitoring system use
10.5.1	Limit viewing of audit trails to those with a job-related need.	A.10.10.3	Protection of log information
10.5.2	Protect audit trail files from unauthorized modifications	A.10.10.3	Protection of log information
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	A.10.10.3	Protection of log information
10.5.4	Write logs for external-facing technologies onto a log server on the internal LAN.	A.10.10.1	Audit Logging
		A.10.1.1	Documented operating procedures

PCI-DSS V1.2 Requirement		ISO 27001 Control	
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.10.10.3	Protection of log information
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.10.10.2	Monitoring system use
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.10.10.3	Protection of log information
Requirement 11 - Regularly test security systems & processes			
11.1	Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	A.12.6.1	Control of technical vulnerabilities
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).	A.12.6.1	Control of technical vulnerabilities
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 subnetwork added to the environment, or a web server added to the environment). These penetration tests must include the following	A.12.6.1	Control of technical vulnerabilities
11.3.1	Network-layer penetration test	A.12.6.1	Control of technical vulnerabilities
11.3.2	Application-layer penetration test	A.12.5.2	Technical review of applications after operating system changes
11.4	Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	A.10.6.2	Security of network services
11.5	Deploy file-integrity monitoring software 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.10.10.2	Monitoring system use

PCI-DSS V1.2 Requirement		ISO 27001 Control	
Maintain an Information Security Policy			
Requirement 12 - Maintain a policy that addresses information security for employees & Contractors			
12.1	Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	A.5.1.1	Information Security Policy Document
12.1.1	Addresses all PCI DSS requirements.	A.15.2.1	Compliance with security policies and standards
12.1.2	Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	A.14.1.2	Business Continuity and Risk Assessment
12.1.3	Includes a review at least once a year and updates when the environment changes.	A.5.1.2	Review of the information security policy
12.2	Develop daily operational security procedures that are consistent with requirements in this specification	A.10.1.1	Documented operating procedures
12-3.	Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	A.7.1.3	Acceptable use of assets
		A.11.7.2	Teleworking
12.3.1	Explicit management approval		
12.3.2	Authentication for use of the technology	A.11.5.2	User identification and authentication
12.3.3	A list of all such devices and personnel with access	A.7.1.1	Inventory of Assets
12.3.4	Labeling of devices with owner, contact information, and purpose	A.7.1.2	Ownership of Assets
		A.11.4.3	Equipment identification in networks
12.3.5	Acceptable uses of the technology	A.7.1.3	Acceptable use of assets
12.3.6	Acceptable network locations for the technologies	A.11.4.1	Policy on use of network services
12.3.7	List of company-approved products	A.7.1.3	Acceptable use of assets
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	A.11.5.5	Session time out
12.3.9	Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use	A.11.4.1	Policy on use of network services

PCI-DSS V1.2 Requirement		ISO 27001 Control	
12.3.10	When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media	A.10.8.1	Information exchange policies and procedures
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	A.6.1.2	Information security coordination
		A.8.1.1	Roles and responsibilities
12.5	Assign to an individual or team the following information security management responsibilities:	A.6.1.3	Allocation of information security responsibilities
12.5.1	Establish, document, and distribute security policies and procedures.	A.5.1	Information Security Policy Document
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel	A.6.1.2	Information security coordination
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations	A.13	Information Security Incident Management
12.5.4	Administer user accounts, including additions, deletions, and modifications	A.6.1.4	Authorization process for information processing facilities
12.5.5	Monitor and control all access to data.	A.10.10	Monitoring
12.6	Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	A.8.2.2	Information security awareness, education and training
12.6.1	Educate employees upon hire and at least annually.	A.8.2.2	Information security awareness, education and training
12.6.2	Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures	A.8.2.2	Information security awareness, education and training
12.7	Screen potential employees	A.8.1.2	Screening
12.8	If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include following	A.6.2.3	Addressing security in third party agreements
		A.6.1.5	Confidentiality agreements
		A.10.2	Third Party Service Management
12.8.1	Maintain a list of service providers	A.10.2.3	Managing changes to third party services
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.	A.6.1.5	Confidentiality agreements

PCI-DSS V1.2 Requirement		ISO 27001 Control	
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	A.6.2.3	Addressing security in third party agreements
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status.	A.10.2.2	Monitoring and review of third party services
12.9	Implement an incident response plan. Be prepared to respond immediately to a system breach	A.13	Information Security Incident Management
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	A.13	Information Security Incident Management
		A.14	Business continuity management
12.9.2	Test the plan at least annually	A.13	Information Security Incident Management
12.9.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	A.13	Information Security Incident Management
12.9.4	Provide appropriate training to staff with security breach response responsibilities.	A.13	Information Security Incident Management
12.9.5	Include alerts from intrusion detection, intrusion-prevention, and file-integrity monitoring systems.	A.10.6.1	Network Controls
		A.10.6.2	Security of network services
12.9.6	Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	A.13	Information Security Incident Management