Mapping between PCI DSS Version 3.1 and ISO/IEC 27002:2013

Introduction

This Mapping Document produced by Orvin Consulting Inc. contains the following tables:

- Table A: a mapping of Payment Card Industry Data Security Standard ("PCI DSS") Version 3.1 Requirements to controls in ISO/IEC 27002:2013 or clauses in ISO/IEC 27001:2013.
- Table B: a mapping of ISO/IEC 27002:2013 controls to PCI DSS Version 3.1 Requirements.

The correspondence between PCI DSS Version 3.1 Requirements and ISO/IEC 27002:2013 controls provided in the Tables are solely the interpretation of Orvin Consulting Inc. There may be other valid interpretations of the correspondence between PCI DSS Version 3.1 Requirements and ISO/IEC 27002:2013 controls.

The PCI Security Standards Council, LLC ("PCI SSC"), the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") have not reviewed this Mapping Document, and have provided no endorsement of its contents.

Target Audience

This document will be useful to users who use ISO/IEC 27002:2013 for their guidance on commonly accepted information security controls, and who are also required to comply with the PCI DSS.

Copyrights

Table A: PCI DSS Version 3.1 Requirements → ISO/IEC 27002:2013 Controls

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	
1.1 Establish and implement firewall and router configuration standards that include the following:	↓ (See below)
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	9.1.2 Access to networks and network services
	14.2.2 System change control procedures
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	12.1.1 Documented operating procedures
	13.1.2 Security of network services
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	12.1.1 Documented operating procedures
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	13.1.3 Segregation in networks
1.1.5 Description of groups, roles, and responsibilities for management of network components	6.1.1 Information security roles and responsibilities
1.1.6 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 v1 and v2.	9.1.2 Access to network and network services
	12.1.1 Documented operating procedures
	13.1.1 Network controls
	13.1.2 Security of network services
	9.1.2 Access to network and network services
	12.1.1 Documented operating procedures
1.1.7 Requirement to review firewall and router rule sets at least every six months	13.1.1 Network controls
	13.1.2 Security of network services
	9.1.2 Access to networks and network services
	14.2.2 System change control procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
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.*	13.1.1 Network controls
	13.1.2 Security of network services
	13.1.3 Segregation in networks
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	13.1.1 Network controls
	13.1.3 Segregation in networks
1.2.2 Secure and synchronize router configuration files [from unauthorized access].	13.1.1 Network controls
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	13.1.1 Network controls
	13.1.3 Segregation in networks
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	13.1.1 Network controls
	13.1.2 Security of network services
	13.1.3 Segregation in networks
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	13.1.1 Network controls
	13.1.3 Segregation in networks
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	13.1.1 Network controls
	13.1.3 Segregation in networks
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	13.1.1 Network controls
	13.1.3 Segregation in networks
1.3.4 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	13.1.1 Network controls
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	13.1.1 Network controls
	13.1.3 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.)	13.1.1 Network controls
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.	13.1.3 Segregation in networks
	14.1.3 Protecting application services transactions

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	13.1.1 Network controls
	13.1.2 Security of network services
1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: • Specific configuration settings are defined for personal firewall software. • Personal firewall software is actively running. • Personal firewall software is not alterable by users of mobile and/or employee-owned devices.	6.2.2 Teleworking
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	6.2.1 Mobile device policy
	12.1.1 Documented operating procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts 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.).	9.2.4 Management of secret authentication information of users
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	9.2.4 Management of secret authentication information of users 13.1.1 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 standards [and are updated as new vulnerability issues are identified]. 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).	9.2.4 Management of secret authentication information of users 12.5.1 Installation of software on operational systems 12.6.1 Management of technical vulnerabilities
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.*	12.5.1 Installation of software on operational systems
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	12.5.1 Installation of software on operational systems

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
2.2.3 Implement additional 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, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.*	13.1.1 Network controls
2.2.4 Configure system security parameters to prevent misuse.	12.5.1 Installation of software on operational systems
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	12.5.1 Installation of software on operational systems
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access. ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.*	13.1.1 Network controls
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	8.1.1 Inventory of assets
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	10.1.1 Policy on the use of cryptographic controls
	12.1.1 Documented operating procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
2.6 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.*	*[See the end of Table A for the ISO/IEC 27002:2013 controls for the PCI DSS Appendix A Requirements]*

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 3: Protect stored cardholder data	
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • 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 process for identifying and securely deleting stored cardholder data that exceeds defined retention.	18.1.3 Protection of records
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *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. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	18.1.3 Protection of records
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) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*	18.1.3 Protection of records
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) after authorization.	18.1.3 Protection of records

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	18.1.3 Protection of records
3.3 Mask PAN 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.*	18.1.3 Protection of records 9.4.1 Information access restriction
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) • Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	8.2.3 Handling of assets 10.1.1 Policy on the use of cryptographic controls 18.1.3 Protection of records
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	8.2.3 Handling of assets 9.1.1 Access control policy 10.1.1 Policy on the use of cryptographic controls 18.1.3 Protection of records
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys— such key-encrypting keys must be at least as strong as the data-encrypting key.*	10.1.1 Policy on the use of cryptographic controls 10.1.2 Key management
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	10.1.2 Key management

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
3.5.2 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method ***Note:*** *It is not required that public keys be stored in one of these forms.*	10.1.2 Key management
3.5.3 Store cryptographic keys in the fewest possible locations.	10.1.2 Key management
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	10.1.2 Key management
3.6.1 Generation of strong cryptographic keys	10.1.2 Key management
3.6.2 Secure cryptographic key distribution	10.1.2 Key management
3.6.3 Secure cryptographic key storage	10.1.2 Key management
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 cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	10.1.2 Key management
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 component), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	10.1.2 Key management

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. ***Note:*** *Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	10.1.2 Key management
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	10.1.2 Key management
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	10.1.2 Key management
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	10.1.1 Policy on the use of cryptographic controls
	12.1.1 Documented operating procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 4: Encrypt transmission of cardholder data across open, public networks	
4.1 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.* *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)* • *General Packet Radio Service (GPRS).* • *Satellite communications.*	10.1.1 Policy on the use of cryptographic controls 13.1.1 Network controls 13.2.3 Electronic messaging 14.1.2 Securing application services on public networks 14.1.3 Protecting application services transactions
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. ***Note:*** *The use of WEP as a security control is prohibited.*	10.1.1 Policy on the use of cryptographic controls 13.1.1 Network controls 13.2.3 Electronic messaging 14.1.2 Securing application services on public networks 14.1.3 Protecting application services transactions
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	8.1.3 Acceptable use of assets 13.2.1 Information transfer policies and procedures 13.2.3 Electronic messaging

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	10.1.1 Policy on the use of cryptographic controls
	12.1.1 Documented operating procedures
	13.2.1 Information transfer policies and procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	12.2.1 Controls against malware
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	12.2.1 Controls against malware
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	12.6.1 Management of technical vulnerabilities
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	12.2.1 Controls against malware
	12.4.1 Event logging
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	12.2.1 Controls against malware
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	6.2.1 Mobile device policy
	10.1.1 Policy on the use of cryptographic controls
	12.1.1 Documented operating procedures
	13.2.1 Information transfer policies and procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 6: Develop and maintain secure systems and applications	
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*	6.1.4 Contact with special interest groups 12.6.1 Management of technical vulnerabilities
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Note:*** *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	12.6.1 Management of technical vulnerabilities
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle ***Note:*** *this applies to all software developed internally as well as bespoke or custom software developed by a third party.*	6.1.5 Information security in project management 14.2.1 Secure development policy 14.2.5 Secure system engineering principles
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	14.2.2 System change control procedures 14.3.1 Protection of test data

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. ***Note:*** *This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	14.2.8 System security testing
	14.2.9 System acceptance testing
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	12.1.2 Change management
	14.2.2 System change control procedures
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	9.1.1 Access control policy
	12.1.4 Separation of development, testing and operational environments
6.4.2 Separation of duties between development/test and production environments	6.1.2 Segregation of duties
6.4.3 Production data (live PANs) are not used for testing or development	14.3.1 Protection of test data
6.4.4 Removal of test data and accounts before production systems become active	14.2.2 System change control procedures
	14.3.1 Protection of test data
6.4.5 Change control procedures for the implementation of security patches and software modifications must include the following:	12.1.2 Change management
	14.2.2 System change control procedures
6.4.5.1 Documentation of impact.	↑ (per 6.4.5 above)
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.	

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. ***Note:*** *The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*	14.2.1 Secure development policy 14.2.5 Secure system engineering principles 14.2.8 System security testing 14.2.9 System acceptance testing
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	↑ (per 6.5 above)
6.5.2 Buffer overflows	
6.5.3 Insecure cryptographic storage	
6.5.4 Insecure communications	
6.5.5 Improper error handling	
6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	
Note: *Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):*	
6.5.7 Cross-site scripting (XSS)	
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	
6.5.9 Cross-site request forgery (CSRF)	
6.5.10 Broken authentication and session management ***Note:*** *Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*	

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 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 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 ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	13.1.1 Network controls
	14.2.3 Technical review of applications after operating platform changes
	18.2.3 Technical compliance review
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	9.1.1 Access control policy
	12.1.1 Documented operating procedures
	14.2.1 Secure development policy
	14.2.2 System change control procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
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.	9.1.1 Access control policy
	9.4.1 Information access restriction
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	9.1.2 Access to networks and network services
	9.4.1 Information access restriction
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	9.1.1 Access control policy
	9.1.2 Access to networks and network services
7.1.3 Assign access based on individual personnel's job classification and function.	9.1.1 Access control policy
	9.4.1 Information access restriction
7.1.4 Require documented approval by authorized parties specifying required privileges.	9.2.3 Management of privileged access rights
7.2 Establish an access control system for systems components 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:	9.1.1 Access control policy
	9.2.2 User access provisioning
	9.4.2 Secure log-on procedures
7.2.1 Coverage of all system components	↑ (per 7.2 above)
7.2.2 Assignment of privileges to individuals based on job classification and function.	
7.2.3 Default "deny-all" setting.	
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	9.1.1 Access control policy
	9.1.2 Access to networks and network services
	9.2.4 Management of secret authentication information of users
	9.2.5 Review of user access rights
	12.1.1 Documented operating procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 8: Identify and authenticate access to system components	
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	↓ (See below)
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	9.2.1 User registration and de-registration
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	9.2.1 User registration and de-registration
	9.2.2 User access provisioning
8.1.3 Immediately revoke access for any terminated users.	9.2.6 Removal or adjustment of access rights
8.1.4 Remove/disable inactive user accounts within 90 days.	9.2.1 User registration and de-registration
8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	9.2.1 User registration and de-registration
	9.2.2 User access provisioning
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	9.4.2 Secure log-on procedures
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	9.4.2 Secure log-on procedures
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	9.4.2 Secure log-on procedures
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing 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.	9.4.2 Secure log-on procedures
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	9.4.2 Secure log-on procedures
	9.4.3 Password management system
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	9.2.4 Management of secret authentication information of users

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
8.2.3 Passwords/phrases must meet the following: • Require a minimum 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.	9.4.3 Password management system
8.2.4 Change user passwords/passphrases at least once every 90 days.	9.4.3 Password management system
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	9.4.3 Password management system
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	9.4.3 Password management system
8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance). ***Note:*** *Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.* *Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.*	9.4.2 Secure log-on procedures
8.4 Document and communicate authentication procedures and policies to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	9.3.1 Use of secret authentication information
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	9.2.1 User registration and de-registration 9.2.3 Management of privileged access rights

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. ***Note:*** *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.* ***Note:*** *Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement.*	9.2.1 User registration and de-registration
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	9.2.1 User registration and de-registration
	9.3.1 Use of secret authentication information
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	9.2.1 User registration and de-registration
	9.3.1 Use of secret authentication information
	9.4.1 Information access restriction
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	9.1.1 Access control policy
	9.1.2 Access to networks and network services
	9.2.1 User registration and de-registration
	9.2.2 User access provisioning
	9.2.4 Management of secret authentication information of users
	9.2.5 Review of user access rights
	12.1.1 Documented operating procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 9: Restrict physical access to cardholder data	
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	11.1.1 Physical security perimeter
	11.1.2 Physical entry controls
	11.1.3 Securing offices, rooms and facilities
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. ***Note:*** *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.* [Video cameras and/or access control mechanisms are protected from tampering or disabling]	11.1.3 Securing offices, rooms and facilities
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	11.1.3 Securing offices, rooms and facilities
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	11.1.3 Securing offices, rooms and facilities
	11.2.3 Cabling security
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying new onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	11.1.2 Physical entry controls
9.3 Control physical access for onsite personnel to the sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	11.1.2 Physical entry controls

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	11.1.2 Physical entry controls
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	↑ (per 9.4 above)
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. 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.	
9.5 Physically secure all media.	8.3.1 Management of removable media
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	8.3.1 Management of removable media
	12.3.1 Information backup
9.6 Maintain strict control over the internal or external distribution of any kind of media [such as paper and electronic media], including the following:	↓ (See below)
9.6.1 Classify media so the sensitivity of the data can be determined.	8.2.1 Classification of information
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	8.3.3 Physical media transfer
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	11.2.5 Removal of assets
9.7 Maintain strict control over the storage and accessibility of media.	8.2.3 Handling of assets
	8.3.1 Management of removable media
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	8.1.1 Inventory of assets

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	8.3.2 Disposal of media
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	8.3.2 Disposal of media
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	8.3.2 Disposal of media 11.2.7 Secure disposal or re-use of equipment
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note:*** *These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.* ***Note:*** *Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.*	6.2.1 Mobile device policy 11.2.6 Security of equipment and assets off-premises 11.2.8 Unattended user equipment
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.	8.1.1 Inventory of assets
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). ***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently coloured casing, or changes to the serial number or other external markings.*	11.2.6 Security of equipment and assets off-premises

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	7.2.2 Information security awareness, education and training
	16.1.2 Reporting information security events
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	11.1.2 Physical entry controls
	12.1.1 Documented operating procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 10: Track and monitor all access to network resources and cardholder data	
10.1 Implement audit trails to link all access to system components to each individual user.	12.4.1 Event logging
10.2 Implement automated audit trails for all system components to reconstruct the following events:	12.4.1 Event logging
10.2.1 All individual user accesses to cardholder data	12.4.1 Event logging
10.2.2 All actions taken by any individual with root or administrative privileges	12.4.3 Administrator and operator logs
10.2.3 Access to all audit trails	12.4.1 Event logging
10.2.4 Invalid logical access attempts	9.4.2 Secure log-on procedures
	12.4.1 Event logging
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	9.2.1 User registration and de-registration
	9.2.2 User access provisioning
	9.2.3 Management of privileged access rights
	12.4.1 Event logging
10.2.6 Initialization, stopping, or pausing of the audit logs	12.4.1 Event logging
10.2.7 Creation and deletion of system-level objects	12.4.1 Event logging
10.3 Record at least the following audit trail entries for all system components for each event:	12.4.1 Event logging
10.3.1 User identification	↑ (per 10.3 above)
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.	
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	12.4.4 Clock synchronisation

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
10.4.1 Critical systems have the correct and consistent time.	↑ (per 10.4 above)
10.4.2 Time data is protected.	
10.4.3 Time settings are received from industry-accepted time sources.	
10.5 Secure audit trails so they cannot be altered.	12.4.2 Protection of log information
10.5.1 Limit viewing of audit trails to those with a job-related need.	12.4.2 Protection of log information
10.5.2 Protect audit trail files from unauthorized modifications.	12.4.2 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.	12.3.1 Information backup
	12.4.2 Protection of log information
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	12.4.2 Protection of log information
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).	12.4.2 Protection of log information
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*	12.4.1 Event logging
	12.4.3 Administrator and operator logs
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	↑ (per 10.6 above)
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	
10.6.3 Follow up exceptions and anomalies identified during the review process.	
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 backup).	16.1.4 Assessment of and decision on information security events

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	12.4.1 Event logging

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 11: Regularly test security systems and processes	
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices [including WLAN cards inserted into system components, and portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.)].*	18.2.3 Technical compliance review
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	8.1.1 Inventory of assets
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	16.1.1 Responsibilities and procedures
	16.1.5 Response to information security incidents
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). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*	18.2.3 Technical compliance review
11.2.1 Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	18.2.3 Technical compliance review

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
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). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	18.2.3 Technical compliance review
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	14.2.3 Technical review of applications after operating platform changes 18.2.3 Technical compliance review
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results. ***Note:*** *This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until version 3 is in place.*	18.2.3 Technical compliance review
11.3.1 Perform external penetration testing at least annually 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).	14.2.3 Technical review of applications after operating platform changes 18.2.3 Technical compliance review

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
11.3.2 Perform internal penetration testing at least annually 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).	14.2.3 Technical review of applications after operating platform changes
	18.2.3 Technical compliance review
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	12.6.1 Management of technical vulnerabilities
	18.2.3 Technical compliance review
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	18.2.3 Technical compliance review
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	12.4.1 Event logging
	13.1.1 Network controls
	13.1.2 Security of network services
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	12.2.1 Controls against malware
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	16.1.4 Assessment of and decision on information security events
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	5.1.1 Policies for information security
	12.1.1 Documented operating procedures
	16.1.1 Responsibilities and procedures

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement 12: Maintain a policy that addresses information security for all personnel	
12.1 Establish, publish, maintain, and disseminate a security policy.	5.1.1 Policies for information security
	7.2.1 Management responsibilities
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	5.1.1 Policies for information security
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. *Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	*[A risk assessment is not defined as a control under ISO/IEC 27002:2013. Risk assessments are one of three main sources of security requirements as described in the section titled "0.2 Information security requirements" of ISO/IEC 27002:2013.]*
12.3 Develop usage policies for critical technologies and define proper use of these technologies. ***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.* Ensure these usage policies require the following:	8.1.3 Acceptable use of assets
12.3.1 Explicit approval by authorized parties	8.2.3 Handling of assets
12.3.2 Authentication for use of the technology	9.4.2 Secure log-on procedures
12.3.3 A list of all such devices and personnel with access	8.1.1 Inventory of assets
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	8.1.2 Ownership of assets
	8.2.2 Labelling of information
12.3.5 Acceptable uses of the technology	7.1.2 Terms and conditions of employment
	8.1.3 Acceptable use of assets
12.3.6 Acceptable network locations for the technologies	11.2.3 Cabling security
	11.2.6 Security of equipment and assets off-premises
	13.1.3 Segregation in networks
12.3.7 List of company-approved products	8.1.1 Inventory of assets

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	9.4.2 Secure log-on procedures
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	9.2.1 User registration and de-registration
	9.2.2 User access provisioning
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	6.2.1 Mobile device policy
	8.3.1 Management of removable media
	13.2.1 Information transfer policies and procedures
12.5 Assign to an individual or team the following information security management responsibilities:	6.1.1 Information security roles and responsibilities
12.5.1 Establish, document, and distribute security policies and procedures.	↑ (per 12.5 above)
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.	
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	7.2.2 Information security awareness, education and training
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	7.2.2 Information security awareness, education and training
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	7.1.2 Terms and conditions of employment
	7.2.1 Management responsibilities

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
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.) ***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	7.1.1 Screening
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	15.1.1 Information security policy for supplier relationships
12.8.1 Maintain a list of service providers.	15.1.1 Information security policy for supplier relationships
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 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.*	13.2.4 Confidentiality or non-disclosure agreements 15.1.2 Addressing security within supplier agreements
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	15.1.1 Information security policy for supplier relationships
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	15.2.1 Monitoring and review of supplier services
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	6.1.1 Information security roles and responsibilities 15.1.2 Addressing security within supplier agreements 15.2.2 Managing changes to supplier services

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
12.9 ***Additional requirement for service providers only:*** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *This requirement is a best practice until June 30, 2015, after which it becomes a requirement.* ***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.*	6.1.1 Information security roles and responsibilities
	15.1.2 Addressing security within supplier agreements
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	16.1.1 Responsibilities and procedures
12.10.1 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 backup 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.	6.1.3 Contact with authorities
	16.1.1 Responsibilities and procedures
	16.1.4 Assessment of and decision on information security events
	16.1.5 Response to information security incidents
	16.1.7 Collection of evidence
	17.1.1 Planning information security continuity
	17.1.3 Verify, review and evaluate information security continuity
	18.1 Compliance with legal and contractual requirements
12.10.2 Test the plan at least annually.	16.1.1 Responsibilities and procedures
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	16.1.1 Responsibilities and procedures
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	16.1.1 Responsibilities and procedures
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	16.1.1 Responsibilities and procedures
	16.1.6 Learning from information security incidents

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	16.1.1 Responsibilities and procedures
	16.1.6 Learning from information security incidents

PCI DSS Version 3.1 Requirement	ISO/IEC 27002:2013 Control
Requirement A.1: Shared hosting providers must protect the cardholder data environment	
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.*	↓ (See below)
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	13.1.3 Segregation in networks
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	9.1.1 Access control policy
	9.1.2 Access to networks and network services
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.	12.4.1 Event logging
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	16.1.1 Responsibilities and procedures

Table B: ISO/IEC 27002:2013 controls → PCI DSS Version 3.1 Requirements

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
5. Information security policies	
5.1.1 Policies for information security	1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.
	2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
	3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.
	4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.
	5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
	6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.
	7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.
	8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
	9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.
	10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.
	11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.
	12.1 Establish, publish, maintain, and disseminate a security policy.
5.1.2 Review of the policies for information security	12.1.1 Review the security policy at least annually and update the policy when the environment changes.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
6. Organization of information security	
6.1.1 Information security roles and responsibilities	1.1.5 Description of groups, roles, and responsibilities for management of network components
	12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
	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.
	12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
	12.9 Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *This requirement is a best practice until June 30, 2015, after which it becomes a requirement.*
6.1.2 Segregation of duties	6.4.2 Separation of duties between development/test and production environments
6.1.3 Contact with authorities	12.10.1 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 *… [See Table A for the full text of this requirement]* • Reference or inclusion of incident response procedures from the payment brands.
6.1.4 Contact with special interest groups	6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. *… [See Table A for the full text of this requirement]*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
6.1.5 Information security in project management	6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle *… [See Table A for the full text of this requirement]*
	12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal risk assessment. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.
6.2.1 Mobile device policy	1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.
	5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
	9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. *… [See Table A for the full text of this requirement]*
	12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.
6.2.2 Teleworking	1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: • Specific configuration settings are defined for personal firewall software. • Personal firewall software is actively running. • Personal firewall software is not alterable by users of mobile and/or employee-owned devices.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
7. Human resource security	
7.1.1 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.) *… [See Table A for the full text of this requirement]*
7.1.2 Terms and conditions of employment	12.3.5 Acceptable uses of the technology
	12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.
7.2.1 Management responsibilities	12.1 Establish, publish, maintain, and disseminate a security policy.
	12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*
7.2.2 Information security awareness, education and training	9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).
	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. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*
7.2.3 Disciplinary process	*[Does not map to any PCI DSS requirements.]*
7.3.1 Termination or change of employment responsibilities	*[Does not map to any PCI DSS requirements, as this control is for defining and communicating the information security responsibilities and duties that remain valid for an employee or contractor after their termination or change of employment.]*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
8. Asset management	
8.1.1 Inventory of assets	2.4 Maintain an inventory of system components that are in scope for PCI DSS.
	9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.
	9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.
	11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.
	12.3.3 A list of all such devices and personnel with access
	12.3.7 List of company-approved products
8.1.2 Ownership of assets	12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)
8.1.3 Acceptable use of assets	4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
	12.3 Develop usage policies for critical technologies and define proper use of these technologies. ***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.* Ensure these usage policies require the following:
	12.3.5 Acceptable uses of the technology
8.1.4 Return of assets	*[Does not map to any PCI DSS requirements.]*
8.2.1 Classification of information	9.6.1 Classify media so the sensitivity of the data can be determined.
8.2.2 Labelling of information	12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
8.2.3 Handling of assets	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) • Strong cryptography with associated key-management processes and procedures. *… [See Table A for the full text of this requirement]*
	3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.
	9.7 Maintain strict control over the storage and accessibility of media.
	12.3.1 Explicit approval by authorized parties
8.3.1 Management of removable media	9.5 Physically secure all media.
	9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.
	9.7 Maintain strict control over the storage and accessibility of media.
	12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. *… [See Table A for the full text of this requirement]*
8.3.2 Disposal of media	9.8 Destroy media when it is no longer needed for business or legal reasons as follows:
	9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.
	9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
8.3.3 Physical media transfer	9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
9. Access control	
9.1.1 Access control policy	3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.
	6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.
	6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.
	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.
	7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.
	7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
	7.1.3 Assign access based on individual personnel's job classification and function.
	7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.
	8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
	A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.
9.1.2 Access to networks and network services	1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations
	1.1.6 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. *… [See Table A for the full text of this requirement]*
(continued on next page)	1.1.7 Requirement to review firewall and router rule sets at least every six months

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
9.1.2 Access to networks and network services (continued from previous page)	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.
	7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.
	7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.
	8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
	A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.
9.2.1 User registration and de-registration	8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.
	8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
	8.1.3 Immediately revoke access for any terminated users.
	8.1.4 Remove/disable inactive user accounts within 90 days.
	8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.
	8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.
(continued on next page)	8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. *… [See Table A for the full text of this requirement]*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
9.2.1 User registration and de-registration (continued from previous page)	8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
	8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).
	8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
	10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
	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
9.2.2 User access provisioning	7.1.4 Require documented approval by authorized parties specifying required privileges.
	8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
	8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.
	8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
	10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
	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

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
9.2.3 Management of privileged access rights	7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
	8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.
	10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
9.2.4 Management of secret authentication information of users	2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. *… [See Table A for the full text of this requirement]*
	2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
	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 [and are updated as new vulnerability issues are identified]. *… [See Table A for the full text of this requirement]*
	7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.
	8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.
	8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
9.2.5 Review of user access rights	7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.
	8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
9.2.6 Removal or adjustment of access rights	8.1.3 Immediately revoke access for any terminated users.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
9.3.1 Use of secret authentication information	8.4 Document and communicate authentication procedures and policies to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.
	8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
	8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).
9.4.1 Information access restriction	3.3 Mask PAN 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. *… [See Table A for the full text of this requirement]*
	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.
	7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.
	7.1.3 Assign access based on individual personnel's job classification and function.
	8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
9.4.2 Secure log-on procedures	7.2 Establish an access control system for systems components 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.
	8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.
	8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
	8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
	8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing 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.
	8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
9.4.3 Password management system	8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
	8.2.3 Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. *… [See Table A for the full text of this requirement]*
	8.2.4 Change user passwords/passphrases at least once every 90 days.
	8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.
	8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
9.4.4 Use of privileged utility programs	*[Does not map to any PCI DSS requirements.]*
9.4.5 Access control to program source code	

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
10. Cryptography	
10.1.1 Policy on the use of cryptographic controls	2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
	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) • Strong cryptography with associated key-management processes and procedures. *… [See Table A for the full text of this requirement]*
	3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.
	3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: *… [See Table A for the full text of this requirement]*
	3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: *… [See Table A for the full text of this requirement]*
	3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.
	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, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *… [See Table A for the full text of this requirement]*

(continued on next page)

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
10.1.1 Policy on the use of cryptographic controls (continued from previous page)	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. ***Note:*** *The use of WEP as a security control is prohibited.*
	4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.
	5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
10.1.2 Key management	3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: *… [See Table A for the full text of this requirement]*
	3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.
	3.5.2 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method ***Note:*** *It is not required that public keys be stored in one of these forms.*
	3.5.3 Store cryptographic keys in the fewest possible locations.
	3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: *… [See Table A for the full text of this requirement]*
	3.6.1 Generation of strong cryptographic keys
	3.6.2 Secure cryptographic key distribution
(continued on next page)	3.6.3 Secure cryptographic key storage

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
10.1.2 Key management (continued from previous page)	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 cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).
	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 component), or keys are suspected of being compromised. *… [See Table A for the full text of this requirement]*
	3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. *… [See Table A for the full text of this requirement]*
	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.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
11. Physical and environmental security	
11.1.1 Physical security perimeter	9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
11.1.2 Physical entry controls	9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
	9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying new onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).
	9.3 Control physical access for onsite personnel to the sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.
	9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:
	9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.
	9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.
	9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.
	9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. *… [See Table A for the full text of this requirement]*
	9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
11.1.3 Securing offices, rooms and facilities	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. *… [See Table A for the full text of this requirement]*
	9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *… [See Table A for the full text of this requirement]*
	9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/ communications hardware, and telecommunication lines.
11.1.4 Protecting against external and environmental threats	*[Does not map to any PCI DSS requirements.]*
11.1.5 Working in secure areas	
11.1.6 Delivery and loading areas	
11.2.1 Equipment siting and protection	
11.2.2 Supporting utilities	
11.2.3 Cabling security	9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/ communications hardware, and telecommunication lines.
	12.3.6 Acceptable network locations for the technologies
11.2.4 Equipment maintenance	*[Does not map to any PCI DSS requirements.]*
11.2.5 Removal of assets	
11.2.6 Security of equipment and assets off-premises	9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. *… [See Table A for the full text of this requirement]*
	9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). *… [See Table A for the full text of this requirement]*
	12.3.6 Acceptable network locations for the technologies

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
11.2.7 Secure disposal or re-use of equipment	9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
11.2.8 Unattended user equipment	9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. *… [See Table A for the full text of this requirement]*
11.2.9 Clear desk and clear screen policy	*[Does not map to any PCI DSS requirements.]*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
12. Operations security	
12.1.1 Documented operating procedures	1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
	1.1.3 Current diagram that shows all cardholder data flows across systems and networks
	1.1.6 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. *… [See Table A for the full text of this requirement]*
	1.1.7 Requirement to review firewall and router rule sets at least every six months
	2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
	3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.
	4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.
	5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
	6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.
	7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.
	8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
	9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.
	10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.
	11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
12.1.2 Change management	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 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.
12.1.3 Capacity management	*[Does not map to any PCI DSS requirements.]*
12.1.4 Separation of development, testing and operational environments	6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.
12.2.1 Controls against malware	5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
	5.1.1 Ensure that 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 maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.
	5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. *… [See Table A for the full text of this requirement]*
	11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *… [See Table A for the full text of this requirement]*
12.3.1 Information backup	9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.
	10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
12.4.1 Event logging	5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.
	10.1 Implement audit trails to link all access to system components to each individual user.
	10.2 Implement automated audit trails for all system components to reconstruct the following events:
	10.2.1 All individual user 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 and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
	10.2.6 Initialization, stopping, or pausing 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.
	10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*

(continued on next page)

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
12.4.1 Event logging (continued from previous page)	10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).
	10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
	10.6.3 Follow up exceptions and anomalies identified during the review process.
	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 backup).
	11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.
	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.
12.4.2 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 secure, centralized, internal log server or media device.
	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).
	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 backup).

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
12.4.3 Administrator and operator logs	10.2.2 All actions taken by any individual with root or administrative privileges
	10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*
	10.6.1 Review the following at least daily: *… [See Table A for the full text of this requirement]* • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).
	10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
	10.6.3 Follow up exceptions and anomalies identified during the review process.
12.4.4 Clock synchronisation	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. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*
	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.
12.5.1 Installation of software on operational systems	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 [and are updated as new vulnerability issues are identified]. *… [See Table A for the full text of this requirement]*
	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.) *… [See Table A for the full text of this requirement]*
	2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
	2.2.4 Configure system security parameters to prevent misuse.
	2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
12.6.1 Management of technical vulnerabilities	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 [and are updated as new vulnerability issues are identified]. *… [See Table A for the full text of this requirement]*
	5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
	6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. *… [See Table A for the full text of this requirement]*
	6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. *… [See Table A for the full text of this requirement]*
	11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.
12.6.2 Restrictions on software installation	*[Does not map to any PCI DSS requirements.]*
12.7.1 Information systems audit controls	

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
13. Communications security	
13.1.1 Network controls	1.1.6 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. *… [See Table A for the full text of this requirement]*
	1.1.7 Requirement to review firewall and router rule sets at least every six months
	1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. *… [See Table A for the full text of this requirement]*
	1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
	1.2.2 Secure and synchronize router configuration files [from unauthorized access].
	1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and 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 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)
	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.)
	1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. *… [See Table A for the full text of this requirement]*

(continued on next page)

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
13.1.1 Network controls (continued from previous page)	2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
	2.2.3 Implement additional 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, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. *… [See Table A for the full text of this requirement]*
	2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access. *… [See Table A for the full text of this requirement]*
	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, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *… [See Table A for the full text of this requirement]*
	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. ***Note:*** *The use of WEP as a security control is prohibited.*
	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 ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.
(continued on next page)	

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
13.1.1 Network controls (continued from previous two pages)	11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.
13.1.2 Security of network services	1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
	1.1.6 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. *… [See Table A for the full text of this requirement]*
	1.1.7 Requirement to review firewall and router rule sets at least every six months
	1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. *… [See Table A for the full text of this requirement]*
	1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.
	1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. *… [See Table A for the full text of this requirement]*
	11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.
13.1.3 Segregation in networks	1.1.4 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. *… [See Table A for the full text of this requirement]*
(continued on next page)	1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
13.1.3 Segregation in networks (continued from previous page)	1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and 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.
	1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
	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.
	12.3.6 Acceptable network locations for the technologies
	A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.
13.2.1 Information transfer policies and procedures	4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
	4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.
	5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
	12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. *… [See Table A for the full text of this requirement]*
13.2.2 Agreements on information transfer	*[Does not map to any PCI DSS requirements.]*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
13.2.3 Electronic messaging	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, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *… [See Table A for the full text of this requirement]*
	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. ***Note:*** *The use of WEP as a security control is prohibited.*
	4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
13.2.4 Confidentiality or non-disclosure agreements	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 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. *… [See Table A for the full text of this requirement]*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
14. System acquisition, development and maintenance	
14.1.1 Information security requirements analysis and specification	*[Does not map to any PCI DSS requirements.]*
14.1.2 Securing application services on public networks	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, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *… [See Table A for the full text of this requirement]*
	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. ***Note:*** *The use of WEP as a security control is prohibited.*
14.1.3 Protecting application services transactions	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.
	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, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *… [See Table A for the full text of this requirement]*
	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. ***Note:*** *The use of WEP as a security control is prohibited.*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
14.2.1 Secure development policy	6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle *… [See Table A for the full text of this requirement]*
	6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. *… [See Table A for the full text of this requirement]*
	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 overflows
	6.5.3 Insecure cryptographic storage
	6.5.4 Insecure communications
	6.5.5 Improper error handling
	6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).
	6.5.7 Cross-site scripting (XSS)
	6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).
	6.5.9 Cross-site request forgery (CSRF)
	6.5.10 Broken authentication and session management ***Note:*** *Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*
	6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
14.2.2 System change control procedures	1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations
	6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.
	6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:
	6.4.4 Removal of test data and accounts before production systems become active
	6.4.5 Change control procedures for the implementation of security patches and software modifications 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.
	6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.
14.2.3 Technical review of applications after operating platform changes	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 ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.
	11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.
	11.3.1 Perform external penetration testing at least annually 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).
	11.3.2 Perform internal penetration testing at least annually 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).

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
14.2.4 Restrictions on changes to software packages	*[Does not map to any PCI DSS requirements.]*
14.2.5 Secure system engineering principles	6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle *… [See Table A for the full text of this requirement]*
	6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. *… [See Table A for the full text of this requirement]*
	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 overflows
	6.5.3 Insecure cryptographic storage
	6.5.4 Insecure communications
	6.5.5 Improper error handling
	6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).
	6.5.7 Cross-site scripting (XSS)
	6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).
	6.5.9 Cross-site request forgery (CSRF)
	6.5.10 Broken authentication and session management ***Note:*** *Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*
14.2.6 Secure development environment	*[Does not map to any PCI DSS requirements.]*
14.2.7 Outsourced development	*[Does not map to any PCI DSS requirements.]*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
14.2.8 System security testing and 14.2.9 System acceptance testing	6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. *… [See Table A for the full text of this requirement]*
	6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. *… [See Table A for the full text of this requirement]*
	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 overflows
	6.5.3 Insecure cryptographic storage
	6.5.4 Insecure communications
	6.5.5 Improper error handling
	6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).
	6.5.7 Cross-site scripting (XSS)
	6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).
	6.5.9 Cross-site request forgery (CSRF)
	6.5.10 Broken authentication and session management ***Note:*** *Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
14.3.1 Protection of test data	6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.
	6.4.3 Production data (live PANs) are not used for testing or development
	6.4.4 Removal of test data and accounts before production systems become active

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
15. Supplier relationships	
15.1.1 Information security policy for supplier relationships	12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:
	12.8.1 Maintain a list of service providers.
	12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
15.1.2 Addressing security within supplier agreements	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 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. *… [See Table A for the full text of this requirement]*
	12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
	12.9 Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *This requirement is a best practice until June 30, 2015, after which it becomes a requirement.*
15.1.3 Information and communication technology supply chain	*[Does not map to any PCI DSS requirements.]*
15.2.1 Monitoring and review of supplier services	12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
15.2.2 Managing changes to supplier services	12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
16. Information security incident management	
16.1.1 Responsibilities and procedures	11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.
	11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.
	12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.
	12.10.1 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 backup 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.
	12.10.2 Test the plan at least annually.
	12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.
	12.10.4 Provide appropriate training to staff with security breach response responsibilities.
	12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.
	12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
	A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.
16.1.2 Reporting information security events	9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: *… [See Table A for the full text of this requirement]* • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
16.1.3 Reporting information security weaknesses	*[Does not map to any PCI DSS requirements.]*
16.1.4 Assessment of and decision on information security events	10.6.3 Follow up exceptions and anomalies identified during the review process.
	11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.
	12.10.1 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 … *[See Table A for the full text of this requirement]* • Coverage and responses of all critical system components …
16.1.5 Response to information security incidents	11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.
	12.10.1 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 backup 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.
16.1.6 Learning from information security incidents	12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.
	12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
16.1.7 Collection of evidence	12.10.1 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 *… [See Table A for the full text of this requirement]* • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components …

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
17. Information security aspects of business continuity management	
17.1.1 Planning information security continuity	12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: *… [See Table A for the full text of this requirement]* • Business recovery and continuity procedures …
17.1.2 Implementing information security continuity	*[Does not map to any PCI DSS requirements.]*
17.1.3 Verify, review and evaluate information security continuity	12.10.1 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 backup 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.
17.2.1 Availability of information processing facilities	*[Does not map to any PCI DSS requirements.]*

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
18. Compliance	
18.1.1 Identification of applicable legislation and contractual requirements	12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: *… [See Table A for the full text of this requirement]* • Analysis of legal requirements for reporting compromises …
18.1.2 Intellectual property rights	*[Does not map to any PCI DSS requirements.]*
18.1.3 Protection of records	3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • 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 process for identifying and securely deleting stored cardholder data that exceeds defined retention.
	3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *… [See Table A for the full text of this requirement]* Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:
	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) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *… [See Table A for the full text of this requirement]*
	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) after authorization.
	3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.
	3.3 Mask PAN 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. *… [See Table A for the full text of this requirement]*

(continued on next page)

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
18.1.3 Protection of records (continued from previous page)	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) • Strong cryptography with associated key-management processes and procedures. *… [See Table A for the full text of this requirement]*
	3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.
18.1.4 Privacy and protection of personally identifiable information	*[Does not map to any PCI DSS requirements.]*
18.1.5 Regulation of cryptographic controls	
18.2.1 Independent review of information security	
18.2.2 Compliance with security policies and standards	
18.2.3 Technical compliance review	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 ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.
	11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. *… [See Table A for the full text of this requirement]*
(continued on next page)	

ISO/IEC 27002:2013 Control	PCI DSS Version 3.1 Requirement
18.2.3 Technical compliance review (continued from previous page)	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). *… [See Table A for the full text of this requirement]*
	11.2.1 Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.
	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). Perform rescans as needed, until passing scans are achieved. *… [See Table A for the full text of this requirement]*
	11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.
	11.3 Implement a methodology for penetration testing that includes the following: *… [See Table A for the full text of this requirement]*
	11.3.1 Perform external penetration testing at least annually 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).
	11.3.2 Perform internal penetration testing at least annually 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).
	11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.
	11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.