PCI DSS 3.1 to 3.2 Requirement Changes

PCI DSS Requirements	Testing Procedures	Guidance
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	1.1.6.a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each. 1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. 1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.	Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don't patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed. Approvals should be granted by personnel independent of the personnel managing the configuration. If insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed. For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (e.g., NIST, ENISA, OWASP, etc.).

Deleted: and

Comment [YD1]: Clarified approvals must be included

Deleted: for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.

Deleted: . ... [1]

Deleted:

Deleted:

Comment [YD2]: This approval addresses Segregation of Duty (SoD) issues.

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	1.2.1.a Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.	Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments. This prevents malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within the entity's network out to an untrusted server). Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.
	1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.	
	1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	1.3 Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment:	While there may be legitimate reasons for untrusted connections to be permitted to DMZ systems (e.g., to allow public access to a web server), such connections should never be granted to systems in the internal network. A firewall's intent is to manage and control all connections between public systems and internal systems, especially those that store, process or transmit cardholder data. If direct access is allowed between public systems and the CDE, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.

Deleted: This requirement is intended to prevent

Comment [YD3]: Clarified that both incoming and outgoing rules must be in place, that is… open only what is required and limit IP ranges and services (protocol/port) and deny everything else.

Deleted: your

Comment [YD4]: Confirm that all external connections must terminate in a DMZ.

Comment [YD5]: 1.3.3 was removed as the PCI SSC left it was already covered.

Deleted: 1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.

Deleted: 1.3.3 Examine firewall and router configurations to verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.

Deleted: Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, as well as inspection and blocking of unwanted content, thus preventing unfiltered access between untrusted and trusted environments. This helps prevent, for example, malicious individuals from sending data they've obtained from within your network out to an external untrusted server in an untrusted network.

1.3.3 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.)	1.3.3 Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ.	Normally a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet came from. Malicious individuals will often try to spoof (or imitate) the sending IP address so that the target system believes the packet is from a trusted source. Filtering packets coming into the network helps to, among other things, ensure packets are not "spoofed" to look like they are coming from an organization's own internal network.
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	1.3.4 Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	All traffic outbound from the cardholder data environment should be evaluated to ensure that it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content).
1.3.5 Permit only "established" connections into the network.	1.3.5 Examine firewall and router configurations to verify that the firewall permits only established connections into the internal network and denies any inbound connections not associated with a previously established session.	A firewall that maintains the "state" (or the status) for each connection through the firewall knows whether an apparent response to a previous connection is actually a valid, authorized response (since it retains each connection's status) or is malicious traffic trying to trick the firewall into allowing the connection.

Comment [YD6]: No change, just renumbered.

Deleted: 4

Deleted: 4

Comment [YD7]: No change, just renumbered.

Deleted: 5

Deleted: 5

Comment [YD8]: Removed "stateful inspection" as there are stronger options available (evaluation left to the assessor). The Verizon 2015 PCI compliance report also points in this direction p.???.

Deleted: 6 Implement stateful inspection, also known as dynamic packet filtering. (That is,

Deleted: 6

Deleted: performs stateful packet inspection

Deleted: are allowed

Deleted: .)

Deleted: the firewall. By maintaining the "state,"

Deleted: performs stateful inspection (dynamic packet filtering). (Only

Deleted: should be allowed in,

Deleted: only if they are

Deleted: .)

1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	1.3.6 Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	If cardholder data is located within the DMZ, it is easier for an external attacker to access this information, since there are fewer layers to penetrate. Securing system components that store cardholder data in an internal network zone that is segregated from the DMZ and other untrusted networks by a firewall can prevent unauthorized network traffic from reaching the system component. Note: This requirement is not intended to apply to temporary storage of cardholder data in volatile memory.
1.3.7 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.	1.3.7.a Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. 1.3.7.b Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized.	Restricting the disclosure of internal or private IP addresses is essential to prevent a hacker "learning" the IP addresses of the internal network, and using that information to access the network. Methods used to meet the intent of this requirement may vary depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.

Comment [YD9]: No change, just renumbered.

Deleted: 7

Deleted: 7

Comment [YD10]: No change, just renumbered.

Deleted: 8

Deleted: 8

Deleted: 8

Deleted:

1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	1.4.a Examine policies and configuration standards to verify: • Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. • Specific configuration settings are defined for personal firewall (or equivalent functionality). • Personal firewall (or equivalent functionality) is configured to actively run. • Personal firewall (or equivalent functionality) is configured to not be alterable by users of the portable computing devices. 1.4.b Inspect a sample of company and/or employee-owned devices to verify that: • Personal firewall (or equivalent functionality) is installed and configured per the organization's specific configuration settings. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	Portable computing devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Internet-based threats. Use of firewall functionality (e.g., personal firewall software or hardware) helps to protect devices from Internet-based attacks, which could use the device to gain access the organization's systems and data once the device is re-connected to the network. The specific firewall configuration settings are determined by the organization. Note: This requirement applies to employee-owned and company-owned portable computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit. Allowing untrusted systems to connect to an organization's CDE could result in access being granted to attackers and other malicious users.

Comment [YD11]: Changed from "mobile" to "portable" since devices that connect remotely (and/or wirelessly) no longer include laptops but smartphones and tablets (and potentially more devices). Personal firewalls in laptops, Mobile Device Management (MDM) generally provide this functionality.

Deleted: mobile

Deleted: devices

Deleted: a

Deleted: mobile

Deleted: devices

Deleted: network

Deleted: network

Deleted: for personal firewall software.

Deleted: software

Deleted: software.

Deleted: The intent of this

Deleted: computers.

Deleted: software

Deleted: software

Deleted: mobile and/or employee-owned

Deleted: to the perimeter

Deleted: software

Deleted: mobile and/or employee-owned

Deleted: network

Deleted: mobile

Deleted: software

Deleted: software

Deleted: software

Deleted: mobile and/or employee-owned

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, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	2.1.a Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.
	2.1.b For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.	

Comment [YD12]: Hardening covers all "system components" which must include applications, not just devices.

Deleted:

	2.1.c Interview personnel and examine supporting documentation to verify that: • All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. • Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.	
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	2.2.3.a Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. 2.2.3.b If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.	Enabling security features before new servers are deployed will prevent servers being installed into the environment with insecure configurations. Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.).
2.3 Encrypt all non-console administrative access using strong cryptography.	2.3 Select a sample of system components and verify that non-console administrative access is encrypted by performing the following:	If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or

Deleted: —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

Deleted: 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. ... [2]

Deleted: 2.2.3.b For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols: ... [4]

Deleted: c For all other environments using SSL and/or

Deleted: : ... [5]

Deleted: being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environ ... [6]

Comment [YD13]: Examples were removed, delegating to NIST for secure protocols (also left to assessors to evaluate). Specific controls for SSL/TLS security is now covered in Appendix A2.

Deleted: place; ... [7]

Deleted: new vulnerabilities associated with

Deleted: early

Deleted: ; ... [8]

Deleted: ... [3]

Deleted: Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.

Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	2.3.a Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.	operational level information (like administrator's IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. To be considered "strong cryptography," industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use. (Refer to "strong cryptography" in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms, and industry standards and best practices such as NIST SP 800-52 and SP 800-57, OWASP, etc.)
	2.3.b Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.	
	2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.	
	2.3.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	
	2.3.e If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.	

Deleted: 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. ... [9]

Comment [YD14]: Examples were removed, delegating to NIST for secure protocols (also left to assessors to evaluate). Specific controls for SSL/TLS security is now covered in Appendix A2.

Comment [YD15]: Added clarification of the risk of passwords being sent in clear-text and potentially captured by an attacker. Ties back to requirement 8.2.1.

Deleted:
2.3.e For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols: ... [11]

Deleted: f For all other environments using SSL and/or

Deleted: : ... [12]

Deleted: being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environ ... [13]

Deleted: ... [10]

Deleted: place; ... [14]

Deleted: new vulnerabilities associated with

Deleted: early

Deleted: ; ... [15]

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 more than the first six/last four digits of the 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.	3.3.a Examine written policies and procedures for masking the display of PANs to verify: • A list of roles that need access to displays of more than the first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that full PAN is only displayed for those with a legitimate business need to see the full PAN minimizes the risk of unauthorized persons gaining access to PAN data. The masking approach should always ensure that only the minimum number of digits is displayed as necessary to perform a specific business function. For example, if only the last four digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last four digits. As another example, if a function needs access to the bank identification number (BIN) for routing purposes, unmask only the BIN digits (traditionally the first six digits) during that function. This requirement relates to protection of PAN displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when stored in files, databases, etc.
	3.3.b Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests.	
	3.3.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see more than the first six/last four digits of the PAN.	

Deleted: full

Deleted: the full

Deleted: other

Comment [YD16]: Clarified that you need to demonstrate what you required and document that justification.

Deleted: full PAN.

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. Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.	3.4.1.a If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account databases or general network login credentials). 3.4.1.b Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls). 3.4.1.c Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored. Note: If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.	The intent of this requirement is to address the acceptability of disk-level encryption for rendering cardholder data unreadable. Disk-level encryption encrypts the entire disk/partition on a computer and automatically decrypts the information when an authorized user requests it. Many disk-encryption solutions intercept operating system read/write operations and carry out the appropriate cryptographic transformations without any special action by the user other than supplying a password or pass phrase upon system startup or at the beginning of a session. Based on these characteristics of disk-level encryption, to be compliant with this requirement, the method cannot: 1) Use the same user account authenticator as the operating system, or 2) Use a decryption key that is associated with or derived from the system's local user account database or general network login credentials. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore may be appropriate for portable devices that store cardholder data.

Comment [YD17]: Added that clarification that if using disk encryption that requirements 3.5.* and 3.6.* must also be performed (this was always the intent).

3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	3.5.1 Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management	Note: This requirement applies only when the entity being assessed is a service provider. Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect cardholder data, as well as the devices that generate, use and protect the keys. This allows an entity to keep pace with evolving threats to their architecture, enabling them to plan for updates as the assurance levels provided by different algorithms/key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices, and identify unauthorized additions to their cryptographic architecture.
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	3.5.2 Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.	There should be very few who have access to cryptographic keys (reducing the potential for rending cardholder data visible by unauthorized parties), usually only those who have key custodian responsibilities.

Comment [YD18]: New documentation requirement for service providers, although this should be applicable to most entities with cryptographic architectures.

Comment [YD19]: No change, just renumbered.

Deleted: 1

Deleted: 1

3.5.3 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.a Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist 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 key components or key shares, in accordance with an industry-accepted method 3.5.3.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one (or more) of the following form at all times. • Encrypted with a key-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As key components or key shares, in accordance with an industry-accepted method	Cryptographic keys must be stored securely to prevent unauthorized or unnecessary access that could result in the exposure of cardholder data. It is not intended that the key-encrypting keys be encrypted, however they are to be protected against disclosure and misuse as defined in Requirement 3.5. If key-encrypting keys are used, storing the key-encrypting keys in physically and/or logically separate locations from the data-encrypting keys reduces the risk of unauthorized access to both keys.

Comment [YD20]: No change, just renumbered.

Deleted: 2

Deleted: 2

Deleted: 2

	3.5.3.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: • Key-encrypting keys are at least as strong as the data-encrypting keys they protect • Key-encrypting keys are stored separately from data-encrypting keys.	
3.5.4 Store cryptographic keys in the fewest possible locations.	3.5.4 Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	Storing cryptographic keys in the fewest locations helps an organization to keep track and monitor all key locations, and minimizes the potential for keys to be exposed to unauthorized parties.
	3.6.1.b Observe the procedures for generating keys to verify that strong keys are generated.	
4.1 Use strong cryptography and security protocols 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: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to: • The Internet	4.1.a Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations. 4.1.b Review documented policies and procedures to verify processes are specified for the following: • For acceptance of only trusted keys and/or certificates • For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported) • For implementation of proper encryption strength per the encryption methodology in use	Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit. Secure transmission of cardholder data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted. Note that some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure versions and

Deleted: 2

Deleted:

Comment [YD21]: No change, just renumbered.

Deleted: 3

Deleted: 3

Comment [YD22]: Change to look at the procedures (which include the method).

Deleted: method

Deleted: (for example, TLS, IPSEC, SSH, etc.)

Deleted: 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. ... [16]

Comment [YD23]: Examples were removed, delegating to NIST for secure protocols (also left to assessors to evaluate). Specific controls for SSL/TLS security is now covered in Appendix A2.

• 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	4.1.c Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit.	configurations to prevent use of an insecure connection—for example, by using only trusted certificates and supporting only strong encryption (not supporting weaker, insecure protocols or methods). Verifying that certificates are trusted (for example, have not expired and are issued from a trusted source) helps ensure the integrity of the secure connection. Generally, the web page URL should begin with "HTTPS" and/or the web browser display a padlock icon somewhere in the window of the browser. Many TLS certificate vendors also provide a highly visible verification seal—sometimes referred to as a “security seal,” "secure site seal," or “secure trust seal”)—which may provide the ability to click on the seal to reveal information about the website. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.)
	4.1.d Examine keys and certificates to verify that only trusted keys and/or certificates are accepted.	
	4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.	
	4.1.f Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	
	4.1.g For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received. For example, for browser-based implementations: • “HTTPS” appears as the browser Universal Record Locator (URL) protocol, and • Cardholder data is only requested if “HTTPS” appears as part of the URL.	
	4.1.h If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.	

Deleted:

Deleted: .

Deleted: ... [17]

Deleted:
4.1.h For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols: ... [18]

Deleted: i For all other environments using SSL and/or

Deleted: : ... [19]

Deleted: being transmitted, types and number of systems that use and/or support SSL/early TLS, type of enviror ... [20]

Deleted: place; ... [21]

Deleted: new vulnerabilities associated with

Deleted: early

Deleted: ; ... [22]

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.	6.2.a Examine policies and procedures related to security-patch installation to verify processes are defined for: • Installation of applicable critical vendor-supplied security patches within one month of release. • Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).	There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system, or gain access to sensitive data. Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months. This requirement applies to applicable patches for all installed software, including payment applications (both those that are PA-DSS validated and those that are not).
	6.2.b For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following: • That applicable critical vendor-supplied security patches are installed within one month of release. • All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).	
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	6.4.4.a Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active.	Test data and accounts should be removed before the system component becomes active (in production), since these items may give away information about the functioning of the application or system. Possession of such information could facilitate compromise of the system and related cardholder data.
	6.4.4.b Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.	

Deleted: .

Comment [YD24]: Updated to ensure that it covers all "system components" which must include applications, not just devices and operating systems.

Comment [YD25]: Again updated to ensure that all system components are covered. Also clarified that these removals must be done before the system goes into production.

Deleted: from production code

Deleted: application

Deleted: systems become active

Deleted: ,

6.4.5 Change control procedures must include the following:	6.4.5.a Examine documented change control procedures and verify procedures are defined for: • Documentation of impact • Documented change approval by authorized parties • Functionality testing to verify that the change does not adversely impact the security of the system • Back-out procedures	If not properly managed, the impact of system changes—such as hardware or software updates and installation of security patches—might not be fully realized and could have unintended consequences.
	6.4.5.b For a sample of system components, interview responsible personnel to determine recent changes. Trace those changes back to related change control documentation. For each change examined, perform the following:	

Deleted: for the implementation of security patches and software modifications

Deleted: related to implementing security patches and software modifications

Deleted:

Comment [YD26]: The changes align with the changes in 6.2 and the new requirement 6.4.6.

Deleted: /security patches.

6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	6.4.6 For a sample of significant changes, examine change records, interview personnel, and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment. Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed. A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through the iterative process. Examples of PCI DSS requirements that could be impacted include, but are not limited to: • Network diagram is updated to reflect changes. • Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. • Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging. • Sensitive authentication data (SAD) is not stored and all cardholder data (CHD) storage is documented and incorporated into data-retention policy and procedures • New systems are included in the quarterly vulnerability scanning process.

Comment [YD27]: This new requirement aims to ensure that the entity maintain compliance with PCI DSS. Any changes that touches on any in-scope "system components" (that list must be maintained per requirement 2.4 and the scope documentation that should be maintained) must be reviewed before approval. A change may affect the scope or the security and this needs to be evaluated before the change takes place.

6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • 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.	6.5.a Examine software-development policies and procedures to verify that up-to-date training in secure coding techniques is required for developers at least annually, based on industry best practices and guidance. 6.5.b Examine records of training to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities. 6.5.c Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities:	The application layer is high-risk and may be targeted by both internal and external threats. Requirements 6.5.1 through 6.5.10 are the minimum controls that should be in place, and organizations should incorporate the relevant secure coding practices as applicable to the particular technology in their environment. Application developers should be properly trained to identify and resolve issues related to these (and other) common coding vulnerabilities. Having staff knowledgeable of secure coding guidelines should minimize the number of security vulnerabilities introduced through poor coding practices. Training for developers may be provided in-house or by third parties and should be applicable for technology used. As industry-accepted secure coding practices change, organizational coding practices and developer training should likewise be updated to address new threats—for example, memory scraping attacks. The vulnerabilities identified in 6.5.1 through 6.5.10 provide a minimum baseline. It is up to the organization to remain up to date with vulnerability trends and incorporate appropriate measures into their secure coding practices.

Deleted: in

Comment [YD28]: 2 important clarifications: the training must be annual (or more often) and it must be updated (since new vector of attacks emerge).

Deleted: , and understanding how sensitive data is handled in memory

Deleted: Interview a sample

Deleted: developers

Deleted: they are knowledgeable in

Deleted: . .

Deleted: 6.5.c Examine records of training to verify that software developers received training on secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.

Deleted:

Deleted: 6.5.d. Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities:

7.2 Establish an access control system(s) 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(s) must include the following:	7.2 Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows:	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.
Requirement 8: Identify and authenticate access to system components		
Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes. The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage. Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). These requirements do not apply to accounts used by consumers (e.g., cardholders). However, Requirements 8.1.1, 8.2, 8.5, 8.2.3 through 8.2.5, and 8.1.6 through 8.1.8 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).		

Comment [YD29]: Clarified that multiple systems could be used (although using the minimum possible is recommended). This is often the case when an environment contains systems that cannot tie into the overall organization directory (Active Directory, LDAP, NIS, etc.) such as specific applications or even the use of mainframes.

Deleted: .

Deleted: An access

Deleted: system automates

Comment [YD30]: Clarification that these requirements applies to the organization users and its third-party users (which act on behalf of the organization).

8.1.5 Manage IDs used by third parties 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.	8.1.5.a Interview personnel and observe processes for managing accounts used by third parties to access, support, or maintain system components to verify that accounts used for remote access are: • Disabled when not in use • Enabled only when needed by the third party, and disabled when not in use. 8.1.5.b Interview personnel and observe processes to verify that third-party remote access accounts are monitored while being used.	Allowing vendors to have 24/7 access into your network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor's environment or from a malicious individual who finds and uses this always-available external entry point into your network. Enabling access only for the time periods needed, and disabling it as soon as it is no longer needed, helps prevent misuse of these connections. Monitoring of vendor access provides assurance that vendors are accessing only the systems necessary and only during approved time frames.
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least	8.2.3a For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	Strong passwords/passphrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID.

Comment [YD31]: Changed from "vendors" to third parties, aligning with requirements 12.8.*.

Deleted: vendors

Deleted: vendors

Deleted: by vendors

Deleted: vendor

Deleted: vendor

Deleted: phrases

Deleted: .

Deleted: phrases

Deleted: phrases

equivalent to the parameters specified above.	8.2.3.b Additional testing procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/passphrases. For cases where this minimum cannot be met due to technical limitations, entities can use "equivalent strength" to evaluate their alternative. For information on variability and equivalency of password strength (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards (e.g., the current version of NIST SP 800-63.) Note: Testing Procedure 8.2.3.b is an additional procedure that only applies if the entity being assessed is a service provider.

Deleted: phrases

Deleted: NIST SP 800-63-1 defines "entropy" as "a measure of the difficulty of guessing or determining a password or key." This document and others that discuss "password entropy" can be referred to for more

Deleted: applicable entropy value and for understanding equivalent

Deleted: variability

Deleted: phrases

Deleted:

Deleted: .

Comment [YD32]: Changed to delegate the detail to the NIST standard.

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. Note: Multi-factor authentication requires that a minimum of 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 multi-factor authentication.		Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication (as described in Requirement 8.2), before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk. Multi-factor authentication is not required at both the system-level and application-level for a particular system component. Multi-factor authentication can be performed either upon authentication to the particular network or to the system component. Examples of multi-factor technologies include but are not limited to remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate multi-factor authentication.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	8.3.1.a Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE.	This requirement is intended to apply to all personnel with administrative access to the CDE. This requirement applies only to personnel with administrative access and

Comment [YD33]: 8.3 in PCI DSS 3.1 is now 8.3.2.
The new 8.3 creates the overall requirement for when multi-factor authentication is required (multi-factor is the renaming of two-factor in previous version of the PCI DSS to align with industry language, but it means the same thing. 2 different types of factors used as described in 8.2).

Comment [YD34]: This new requirement is something I and many others have called for since "with great power comes great responsibility". All administrators logging in remotely to CDE systems must be using multi-factor authentication. My recommendation is that all management be performed using dedicated systems (can be VMs) located within secure zone and that the access to these dedicated management systems is where multi-factor authentication be implemented.

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	8.3.1.b Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used.	only for non-console access to the CDE; it does not apply to application or system accounts performing automated functions. If the entity does not use segmentation to separate the CDE from the rest of their network, an administrator could use multi-factor authentication either when logging onto the CDE network or when logging onto a system. If the CDE is segmented from the rest of the entity's network, an administrator would need to use multi-factor authentication when connecting to a CDE system from a non-CDE network. Multi-factor authentication can be implemented at network level or at system/application level; it does not have to be both. If the administrator uses MFA when logging into the CDE network, they do not also need to use MFA to log into a particular system or application within the CDE.
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	8.3.2.a Examine system configurations for remote access servers and systems to verify multi-factor authentication is required for: • All remote access by personnel, both user and administrator, and • All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes).	This requirement is intended to apply to all personnel—including general users, administrators, and vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the CDE. If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data

Deleted: two

Deleted: Two-factor authentication requires two forms of authentication for higher-risk accesses, such as those originating from outside the network

Deleted: originating from outside the network by personnel (

Deleted: users and administrators) and all

Deleted: parties, (including vendor

Deleted: two

Deleted:). ... [23]

Comment [YD35]: This was 8.3 before and only changed for multi-factor language.

Deleted: cardholder data environment.

Deleted:

	8.3.2.b Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used.	environment, multi-factor authentication for remote access to that network would not be required. However, multi-factor authentication is required for any remote access to networks with access to the cardholder data environment, and is recommended for all remote access to the entity's networks.
9.1.1 Use either video cameras or access control mechanisms (or both) 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.	9.1.1.a Verify that either video cameras or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas. 9.1.1.b Verify that either video cameras or access control mechanisms (or both) are protected from tampering or disabling. 9.1.1.c Verify that data from video cameras and/or access control mechanisms is reviewed, and that data is stored for at least three months.	When investigating physical breaches, these controls can help identify the individuals that physically accessed the sensitive areas, as well as when they entered and exited. Criminals attempting to gain physical access to sensitive areas will often attempt to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, access control mechanisms could be monitored or have physical protections installed to prevent them being damaged or disabled by malicious individuals. Examples of sensitive areas include corporate database server rooms, back-office rooms at retail locations that store cardholder data, and storage areas for large quantities of cardholder data. Sensitive areas should be identified by each organization to ensure the appropriate physical monitoring controls are implemented.

Deleted: two

Deleted: two

Comment [YD36]: Clarified that while you can use both, you are only mandated to use one.

Deleted: and/

Deleted: and/

Deleted:

Deleted: and/

Deleted:

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	9.5.1 Verify that the storage location security is reviewed at least annually to confirm that backup media storage is secure.	If stored in a non-secured facility, backups that contain cardholder data may easily be lost, stolen, or copied for malicious intent. Periodically reviewing the storage facility enables the organization to address identified security issues in a timely manner, minimizing the potential risk.
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	10.8.a Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) 10.8.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	Note: This requirement applies only when the entity being assessed is a service provider. Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment. The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.

Deleted: .a Observe

Deleted: location's physical

Comment [YD37]: Combined 2 test procedures.

Moved (insertion) [1]

Deleted: 9.5.1.b Verify that the storage location security is reviewed at least annually.

Moved up [1]: Periodically reviewing the storage facility enables the organization to address identified security issues in a timely manner, minimizing the potential risk.

Deleted: 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.

Deleted: documentation and interview personnel to verify that security

Deleted: Personnel need

Deleted: operational

Deleted: monitoring all

Deleted: be aware of

Deleted: following

Deleted: policies

Comment [YD38]: New requirement for service providers that ties back to requirement A3.3.1 in Appendix A3 (previously in DESV).

Deleted: daily operational procedures for monitoring all access

Deleted: network resources

Deleted: a continuous basis

Deleted: to network resources and cardholder data are:

Deleted: <#>Documented, ... [24]

10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	10.8.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls 10.8.1.b Examine records to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	Note: This requirement applies only when the entity being assessed is a service provider. If critical security control failures alerts are not quickly and effectively responded to, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. Documented evidence (e.g., records within a problem management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk"	11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.	An established process for identifying vulnerabilities on internal systems requires that vulnerability scans be conducted

Comment [YD39]: New requirement for service providers that ties back to requirement A3.3.1.1 in Appendix A3 (previously in DESV).

Deleted:

Deleted: as needed, until

Deleted: -

vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	11.2.1.b Review the scan reports and verify that all "high risk" vulnerabilities are addressed and the scan process includes rescans to verify that the "high risk" vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved.	quarterly. Vulnerabilities posing the greatest risk to the environment (for example, ranked "High" per Requirement 6.1) should be resolved with the highest priority.
	11.2.1.c Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a firewall administrator should not be responsible for scanning the firewall), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.
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.	11.3.4.a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Penetration testing is an important tool to confirm that any segmentation in place to isolate the CDE from other networks is effective. The penetration testing should focus on the segmentation controls, both from outside the entity's network and from inside the network but outside of the CDE, to confirm that they are not able to get through the segmentation controls to access the CDE. For example, network testing and/or scanning for open ports, to verify no connectivity between in-scope and out-of-scope networks.
	11.3.4.b Examine the results from the most recent penetration test to verify that: • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	

Deleted: (as identified

Deleted:) are resolved.

Comment [YD40]: Clarified that the risk ranking to use is the one used for 6.1, and the vulnerabilities must be resolved and that we must confirm that they were indeed resolved (by rescanning).

Deleted: until all

Deleted: -

Deleted: ,

	11.3.4.c Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	11.3.4.1.a Examine the results from the most recent penetration test to verify that: • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Note: This requirement applies only when the entity being assessed is a service provider. For service providers, validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives.
	11.3.4.1.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	

Comment [YD41]: Added requirement on whom is performing the task. Must be qualified to perform the testing and be independent (no conflict of interest, segregation of duties issue).

Comment [YD42]: New requirement for service providers that ties back to requirement A3.2.4 in Appendix A3 (previously in DESV).

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).	11.5.a Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files • Additional critical files determined by entity (for example, through risk assessment or other means).	Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.
12.3.3 A list of all such devices and personnel with access	12.3.3 Verify that the usage policies define • A list of all critical devices, and • A list of personnel authorized to use the devices.	Malicious individuals may breach physical security and place their own devices on the network as a "back door." Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	12.4.a Verify that information security policies clearly define information security responsibilities for all personnel. 12.4.b Interview a sample of responsible personnel to verify they understand the security policies.	Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to unsecured implementation of technologies or use of outdated or unsecured technologies.

Comment [YD43]: This test procedure used to imply that this requirement only applied to CDE systems (not connected ones). Its removal means that all in-scope systems should now be covered.

Deleted: within the cardholder data environment

Deleted: a

Comment [YD44]: Clarified that this applies to critical devices (TBD by the organization) and personnel that accesses these devices.
End-user accesses are covered by requirements 7 and 8.

12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	12.4.1.a Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance. 12.4.1.b Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.	Note: This requirement applies only when the entity being assessed is a service provider. Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization. Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure. The level of detail provided to executive management should be appropriate for the particular organization and the intended audience.
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	12.6.a Review the security awareness program to verify it provides awareness to all personnel about the cardholder data security policy and procedures . 12.6.b Examine security awareness program procedures and documentation and perform the following:	If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.
12.8.1 Maintain a list of service providers including a description of the service provided.	12.8.1 Verify that a list of service providers is maintained and includes a description of the service provided.	Keeping track of all service providers identifies where potential risk extends to outside of the organization.

Comment [YD45]: New requirement for service providers that ties back to requirement A3.1.1 in Appendix A3 (previously in DESV).

Deleted: importance of

Deleted: importance of

Comment [YD46]: Updated to ensure that not just security of card information is covered but of the organization's policies and procedures (i.e. what to do if I come across card information).

Comment [YD47]: Clarified that the services offered must also be described. Ties back to 12.8.5 and 12.9.

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.	12.8.2 Observe written agreements and confirm they include an acknowledgement by service providers that they 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.	The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity. In conjunction with Requirement 12.9, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.	12.10.2 Interview personnel and review documentation from testing to verify that the plan is tested at least annually, and that testing includes all elements listed in Requirement 12.10.1.	Without proper testing, key steps may be missed, which could result in increased exposure during an incident.
12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	12.11.a Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	Note: This requirement applies only when the entity being assessed is a service provider. Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The objective of these reviews is not to re-perform other PCI DSS requirements, but to confirm whether procedures are being followed as expected.

Deleted: for written agreements between organizations and service provides

Deleted: Test

Deleted: Verify

Comment [YD48]: Clarified that a review must occur in addition to the testing.

Comment [YD49]: Clarified that the full plan (all possibilities) must be tested. This could be a simple table top.

Comment [YD50]: New requirement for service providers that ties back to requirement A3.3.3 in Appendix A3 (previously in DESV).

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	12.11.b Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly.	
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	12.11.1 Examine documentation from the quarterly reviews to verify they include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	Note: This requirement applies only when the entity being assessed is a service provider. The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for its next PCI DSS assessment.

Comment [YD51]: See 12.11.1

Page 1: [1] Deleted	v.3.2	6/16/16 11:11:00 AM

Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.

Page 7: [2] Deleted	v.3.2	6/16/16 11:11:00 AM

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.

Page 7: [3] Deleted	v.3.2	6/16/16 11:11:00 AM

Regarding use of SSL/early TLS: Entities using SSL and early TLS must work towards upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where they don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

Refer to the PCI SSC Information Supplement Migrating from SSL and Early TLS for further guidance on the use of SSL/early TLS.

Page 7: [4] Deleted	v.3.2	6/16/16 11:11:00 AM

	2.2.3.b For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols: Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	

Page 7: [5] Deleted	v.3.2	6/16/16 11:11:00 AM

:

Review the documented Risk Mitigation and Migration Plan to verify it includes:

Description of usage, including what data

Page 7: [6] Deleted	v.3.2	6/16/16 11:11:00 AM

being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;

Risk-assessment results and risk-reduction controls

Page 7: [7] Deleted	v.3.2	6/16/16 11:11:00 AM

place;

Description of processes to monitor

Page 7: [8] Deleted	v.3.2	6/16/16 11:11:00 AM

;

Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;

Overview of migration project plan including target migration completion date no later than June 30, 2016

Page 8: [9] Deleted	v.3.2	6/16/16 11:11:00 AM

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.

Page 8: [10] Deleted	v.3.2	6/16/16 11:11:00 AM

Regarding use of SSL/early TLS: Entities using SSL and early TLS must work towards upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where they don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

Refer to the PCI SSC Information Supplement Migrating from SSL and Early TLS for further guidance on the use of SSL/early TLS.

Page 8: [11] Deleted	v.3.2	6/16/16 11:11:00 AM

	2.3.e For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols: Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	

Page 8: [12] Deleted **v.3.2** **6/16/16 11:11:00 AM**

:

Review the documented Risk Mitigation and Migration Plan to verify it includes:

Description of usage, including what data

Page 8: [13] Deleted **v.3.2** **6/16/16 11:11:00 AM**

being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;

Risk-assessment results and risk-reduction controls

Page 8: [14] Deleted **v.3.2** **6/16/16 11:11:00 AM**

place;

Description of processes to monitor

Page 8: [15] Deleted **v.3.2** **6/16/16 11:11:00 AM**

;

Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;

Overview of migration project plan including target migration completion date no later than June 30, 2016

Page 13: [16] Deleted **v.3.2** **6/16/16 11:11:00 AM**

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.

Page 14: [17] Deleted **v.3.2** **6/16/16 11:11:00 AM**

Regarding use of SSL/early TLS: Entities using SSL and early TLS must work towards upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where they don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

Refer to the PCI SSC Information Supplement: Migrating from SSL and Early TLS for further guidance on the use of SSL/early TLS.

Page 14: [18] Deleted **v.3.2** **6/16/16 11:11:00 AM**

	4.1.h For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols: Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	

Page 14: [19] Deleted **v.3.2** **6/16/16 11:11:00 AM**

:

Review the documented Risk Mitigation and Migration Plan to verify it includes:

Description of usage, including what data

Page 14: [20] Deleted **v.3.2** **6/16/16 11:11:00 AM**

being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;

Risk-assessment results and risk-reduction controls

Page 14: [21] Deleted **v.3.2** **6/16/16 11:11:00 AM**

place;

Description of processes to monitor

Page 14: [22] Deleted **v.3.2** **6/16/16 11:11:00 AM**

;

Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;

Overview of migration project plan including target migration completion date no later than June 30, 2016

Page 23: [23] Deleted	v.3.2	6/16/16 11:11:00 AM

).

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

Page 25: [24] Deleted	v.3.2	6/16/16 11:11:00 AM

Documented,

In use, and

Known to all affected parties.

·