## Build and Maintain a Secure Network and Systems

### Requirement 1: Install and maintain a firewall configuration to protect cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings** (check one) | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | | **N/A** | **Not Tested** | **Not in Place** |
| **1.1** Establish and implement firewall and router configuration standards that include the following: | | | | | | | | |
| **1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows: | | | | | | | | |
| **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all:   * Network connections, and * Changes to firewall and router configurations. | **Identify the document(s)** reviewed to verify procedures define the formal processes for: | | | | | | | |
| * Testing and approval of all network connections. |  | | | | | | |
| * Testing and approval of all changes to firewall and router configurations. |  | | | | | | |
| **1.1.1.b** For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested. | **Identify the sample of records** for network connections that were examined. |  | | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that network connections were approved and tested. |  | | | | | | |
| **Describe how** the sampled records were examined to verify that network connections were: | | | | | | | |
| * Approved |  | | | | | | |
| * Tested |  | | | | | | |
| **1.1.1.c** Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested. | **Identify** **the sample of records** for firewall and router configuration changes that were examined. |  | | | | | | |
| **Identify** **the responsible personnel** interviewed who confirm that changes made to firewall and router configurations were approved and tested. |  | | | | | | |
| **Describe how** change records were compared to actual changes made to firewall and router configurations to verify the changes were: | | | | | | | |
| * Approved |  | | | | | | |
| * Tested |  | | | | | | |
| **1.1.2** Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to the cardholder data environment, including any wireless networks. | **Identify the current network diagram**(s) examined. |  | | | | | | |
| **Describe how** network connections were observed and compared to the diagram(s) to verify that the diagram: | | | | | | | |
| * Is current. |  | | | | | | |
| * Includes all connections to cardholder data. |  | | | | | | |
| * Includes any wireless network connections. |  | | | | | | |
| **1.1.2.b** Interview responsible personnel to verify that the diagram is kept current. | **Identify** **the document** examined to verify processes require that the network diagram is kept current. |  | | | | | | |
| **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that the diagram is kept current. |  | | | | | | |
| **1.1.3** Current diagram that shows all cardholder data flows across systems and networks. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.3.a** Examine data flow diagram and interview personnel to verify the diagram:   * Shows all cardholder data flows across systems and networks. * Is kept current and updated as needed upon changes to the environment. | **Identify** **the data-flow diagram**(s) examined. |  | | | | | | |
| **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify the diagram: | | | | | | | |
| * Shows all cardholder data flows across systems and networks. |  | | | | | | |
| * Is kept current and updated as needed upon changes to the environment. |  | | | | | | |
| **1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.4.a** Examine thefirewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. | **Identify** **the firewall configuration standards document** examined to verify requirements for a firewall:   * At each Internet connection. * Between any DMZ and the internal network zone. |  | | | | | | |
| **1.1.4.b** Verify that the current network diagram is consistent with the firewall configuration standards. | **Provide the name of the assessor** who attests that the current network diagram identified at 1.1.2.a was compared to the firewall configuration standards identified at 1.1.4.a to verify they are consistent with each other. |  | | | | | | |
| **1.1.4.c** Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams. | **Describe how** network configurations were observed to verify that, per the documented configuration standards and network diagrams, a firewall is in place: | | | | | | | |
| * At each Internet connection. |  | | | | | | |
| * Between any DMZ and the internal network zone. |  | | | | | | |
| **1.1.5** Description of groups, roles, and responsibilities for management of network components. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components. | **Identify** **the firewall and router configuration standards document(s)** reviewed to verify they include a description of groups, roles and responsibilities for management of network components. |  | | | | | | |
| **1.1.5.b** Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented. | **Identify the personnel** responsible for management of network components interviewed for this testing procedure. |  | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that roles and responsibilities are assigned as documented for management of firewall and router components. |  | | | | | | |
| **1.1.6** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.  Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols. | **Identify** **the firewall configuration standards document(s)** reviewed to verify the document(s) contains a list of all services, protocols and ports necessary for business, including a business justification for each. |  | | | | | | |
| **Identify** **the router configuration standards document(s)** reviewed to verify the document contains a list of all services, protocols and ports necessary for business, including a business justification for each. |  | | | | | | |
| **1.1.6.b** Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. | **Indicate whether** any insecure services, protocols or ports are allowed. **(yes/no)** |  | | | | | | |
| *If “yes,” complete the instructions below for EACH insecure service, protocol, and port allowed: (add rows as needed)* | | | | | | | |
| **Identify** the documented justification. |  | | | | | | |
| **Identify the firewall and router configuration standards** reviewed to verify that security features are documented for each insecure service/protocol/port. |  | | | | | | |
| **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. | *If “yes” at 1.1.6.b, complete the following for each insecure service, protocol, and/or port present (add rows as needed):* | | | | | | | |
| **Describe how** the firewall and router configurations were examined to verify that the documented security features are implemented for each insecure service, protocol and/or port. |  | | | | | | |
| **1.1.7** Requirement to review firewall and router rule sets at least every six months. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.1.7.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. | **Identify** **the firewall and router configuration standards** reviewed to verify they require a review of firewall rule sets at least every six months. |  | | | | | | |
| **1.1.7.b** Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months. | **Identify the document(s) relating to rule set reviews** that were examined to verify that rule sets are reviewed at least every six months for firewall and router rule sets. |  | | | | | | |
| **Identify the responsible personnel interviewed** who confirm that rule sets are reviewed at least every six months for firewall and router rule sets. |  | | | | | | |
| **1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.  **Note:** An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. | | | | | | | | |
| **1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment: | | | | | | | | |
| **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. | **Identify the firewall and router configuration standards** reviewed to verify they identify inbound and outbound traffic necessary for the cardholder data environment. |  | | | | | | |
| **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. | **Describe how** firewall and router configurations were examined to verify that the following traffic is limited to that which is necessary for the cardholder data environment: | | | | | | | |
| * Inbound traffic |  | | | | | | |
| * Outbound traffic |  | | | | | | |
| **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. | **Describe how** firewall and router configurations were examined to verify the following is specifically denied: | | | | | | | |
| * All other inbound traffic |  | | | | | | |
| * All other outbound traffic |  | | | | | | |
| **1.2.2** Secure and synchronize router configuration files. | | | ☐ | | ☐ | ☐ | ☐ | ☐ |
| **1.2.2.a** Examine router configuration files to verify they are secured from unauthorized access. | **Describe how** router configuration files were examined to verify they are secured from unauthorized access. |  | | | | | | |
| **1.2.2.b** Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted). | **Describe how** router configuration files were examined to verify they are synchronized. |  | | | | | | |
| **1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.2.3.a** Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment. | **Describe how** firewall and router configurations were examined to verify perimeter firewalls are in place between all wireless networks and the cardholder data environment. |  | | | | | | |
| **1.2.3.b** Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | **Indicate whether** traffic between the wireless environment and the cardholder data environment is necessary for business purposes. **(yes/no)** |  | | | | | | |
| *If “no”:* | | | | | | | |
| **Describe how** firewall and/or router configurations were observed to verify firewalls deny all traffic from any wireless environment into the cardholder environment. |  | | | | | | |
| *If “yes”:* | | | | | | | |
| **Describe how** firewall and/or router configurations were observed to verify firewalls permit only authorized traffic from any wireless environment into the cardholder environment. |  | | | | | | |
| **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: | | | | | | | | |
| **1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.1** Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | **Describe how** the firewall and router configurations were examined to verify that the DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. |  | | | | | | |
| **1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ. | **Describe how** thefirewall and router configurations were examined to verify that configurations limit inbound Internet traffic to IP addresses within the DMZ. |  | | | | | | |
| **1.3.3** Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.3** 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. | **Describe how** the examined firewall and router configurations were observed to prevent direct connections between the Internet and the cardholder data environment: | | | | | | | |
| * Inbound |  | | | | | | |
| * Outbound |  | | | | | | |
| **1.3.4** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.  (For example, block traffic originating from the Internet with an internal source address) | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.4** 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**.** | **Describe how** firewall and router configurations were examined to verify that anti-spoofing measures are implemented. |  | | | | | | |
| **Describe** the anti-spoofing measures implemented |  | | | | | | |
| **1.3.5** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.5** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. | **Describe how** firewall and router configurations were examined to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. |  | | | | | | |
| **1.3.6** Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.) | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.6** Examine firewall and router configurations to verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.) | **Describe how** firewall and router configurations were examined to verify that the firewall performs stateful inspection. |  | | | | | | |
| **Describe** how observed firewall configurations implement stateful inspection |  | | | | | | |
| **1.3.7** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.7** 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. | **Indicate whether** any system components store cardholder data. **(yes/no)** |  | | | | | | |
| *If “yes”:* | | | | | | | |
| **Describe how** firewall and router configurations were examined to verify that the system components that store cardholder data are located on an internal network zone, and are segregated from the DMZ and other untrusted networks. |  | | | | | | |
| **1.3.8** Do not disclose private IP addresses and routing information to unauthorized parties.  Note: Methods to obscure IP addressing may include, but are not limited to:   * Network Address Translation (NAT), * Placing servers containing cardholder data behind proxy servers/firewalls, * Removal or filtering of route advertisements for private networks that employ registered addressing, * Internal use of RFC1918 address space instead of registered addresses. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.3.8.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. | **Describe** the methods in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. |  | | | | | | |
| **Describe how** firewall and router configurations were examined to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. |  | | | | | | |
| **1.3.8.b** Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized. | **Identify the document** reviewed that specifies whether any disclosure of private IP addresses and routing information to external parties is permitted. |  | | | | | | |
| For each permitted disclosure, **identify the responsible personnel** interviewed who confirm that the disclosure is authorized. |  | | | | | | |
| **1.4** Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include:   * Specific configuration settings are defined for personal firewall software. * Personal firewall software is actively running. * Personal firewall software is not alterable by users of mobile and/or employee-owned devices. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.4.a** Examinepolicies andconfiguration standards to verify:   * Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the network. * Specific configuration settings are defined for personal firewall software. * Personal firewall software is configured to actively run. * Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices. | **Indicate whether** mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network are used to access the organization’s network. **(yes/no)** |  | | | | | | |
| *If “no,”* **identify** **the document** reviewed that explicitly prohibits mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network from being used to access the organization’s network.  *Mark 1.4.b as “not applicable”* |  | | | | | | |
| *If “yes,”* **identify** **the documented policies and configuration standards** that define the following:   * Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet when outside the network, and which are also used to access the network. * Specific configuration settings are defined for personal firewall software. * Personal firewall software is configured to actively run. * Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices. |  | | | | | | |
| **1.4.b** Inspect a sample of mobile and/or employee-owned devices to verify that:   * Personal firewall software is installed and configured per the organization’s specific configuration settings. * Personal firewall software is actively running. * Personal firewall software is not alterable by users of mobile and/or employee-owned devices. | **Identify the sample** of mobile and/or employee-owned devices selected for this testing procedure. |  | | | | | | |
| **Describe how** the sample of mobile and/or employee-owned devices was inspected to verify that personal firewall software is: | | | | | | | |
| * Installed and configured per the organization’s specific configuration settings. |  | | | | | | |
| * Actively running. |  | | | | | | |
| * Not alterable by users of mobile and/or employee-owned devices. |  | | | | | | |
| **1.5** Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. | | | ☐ | ☐ | | ☐ | ☐ | ☐ |
| **1.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed** to verify that security policies and operational procedures for managing firewalls are documented. |  | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for managing firewalls are:   * In use * Known to all affected parties |  | | | | | | |

### Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **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, POS terminals, 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.) | **Identify the sample** of system components selected. |  | | | | | |
| **Identify** **the vendor manuals and sources on the Internet** used to find vendor-supplied accounts/passwords. |  | | | | | |
| *For each item in the sample*, **describe how** attempts to log on (with system administrator help) to the sample of devices and applications using default vendor-supplied accounts and passwords were performed to verify that all default passwords have been changed. |  | | | | | |
| **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. | *For each item in the sample of system components indicated at 2.1.a,* ***describe how*** *all unnecessary default accounts were verified to be* ***either****:* | | | | | | |
| * Removed |  | | | | | |
| * Disabled |  | | | | | |
| **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. | **Identify responsible personnel** interviewed who 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. |  | | | | | |
| **Identify supporting documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** the supporting documentation examined verified that: | | | | | | |
| * All vendor defaults are changed before a system is installed on the network. |  | | | | | |
| * Unnecessary default accounts are removed or disabled before a system is installed on the network. |  | | | | | |
| **2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.1.1.a** Interview responsible personnel and examine supporting documentation to verify that:   * Encryption keys were changed from default at installation * Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. | **Indicate whether** there are wireless environments connected to the cardholder data environment or transmitting cardholder data. **(yes/no)**  *If “no,” mark 2.1.1 as “Not Applicable” and proceed to 2.2.* |  | | | | | |
| *If “yes”:* | | | | | | |
| **Identify responsible personnel** interviewed who verify that encryption keys are changed:   * From default at installation * Anytime anyone with knowledge of the keys leaves the company or changes positions. |  | | | | | |
| **Identify supporting documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** the supporting documentation was examined to verify that encryption keys are changed: | | | | | | |
| * From default at installation |  | | | | | |
| * Anytime anyone with knowledge of the keys leaves the company or changes positions. |  | | | | | |
| **2.1.1.b** Interview personnel and examine policies and procedures to verify:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. | **Identify responsible personnel** interviewed who verify that:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. |  | | | | | |
| **Identify policies and procedures** examined to verify that:   * Default SNMP community strings are required to be changed upon installation. * Default passwords/phrases on access points are required to be changed upon installation. |  | | | | | |
| **2.1.1.c** Examine vendor documentation and login to wireless devices, with system administrator help, to verify:   * Default SNMP community strings are not used. * Default passwords/passphrases on access points are not used. | **Identify** **vendor documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** examined vendor documentation was usedto attempt to login to wireless devices (with system administrator help) to verify: | | | | | | |
| * Default SNMP community strings are not used. |  | | | | | |
| * Default passwords/passphrases on access points are not used. |  | | | | | |
| **2.1.1.d** Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for:   * Authentication over wireless networks * Transmission over wireless networks | **Identify** **vendor documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** wireless configuration settings were observed with examined vendor documentation to verify that firmware on wireless devices is updated to support strong encryption for: | | | | | | |
| * Authentication over wireless networks. |  | | | | | |
| * Transmission over wireless networks. |  | | | | | |
| **2.1.1.e** Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable. | **Identify** **vendor documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** wireless configuration settings were observed with examined vendor documentation to verify other security-related wireless vendor defaults were changed, if applicable. |  | | | | | |
| **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.  Sources of industry-accepted system hardening standards may include, but are not limited to:   * Center for Internet Security (CIS) * International Organization for Standardization (ISO) * SysAdmin Audit Network Security (SANS) Institute * National Institute of Standards Technology (NIST) | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.a** Examine the organization’s system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. | **Identify** **the documented system configuration standards** for all types of system components examined. |  | | | | | |
| **Identify** **the industry-accepted hardening standards** the system configuration standards were verified to be consistent with. |  | | | | | |
| **2.2.b** Examine policies and interview personnel toverify thatsystem configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1. | **Identify** **the policy documentation** verified to define that system configuration standards are updated as new vulnerability issues are identified |  | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that the process is implemented. |  | | | | | |
| **2.2.c** Examine policies and interview personnel toverify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. | **Identify** **the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network |  | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify: | | | | | | |
| * System configuration standards are applied when new systems are configured |  | | | | | |
| * System configuration standards are verified as being in place before a system is installed on the network. |  | | | | | |
| **2.2.d** Verify that system configuration standards include the following procedures for all types of system components:   * Changing of all vendor-supplied defaults and elimination of unnecessary default accounts * Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server * Enabling only necessary services, protocols, daemons, etc., as required for the function of the system * Implementing additional security features for any required services, protocols or daemons that are considered to be insecure * Configuring system security parameters to prevent misuse * Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers | **Identify the system configuration standards** for all types of system components that include the following procedures:   * Changing of all vendor-supplied defaults and elimination of unnecessary default accounts * Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server * Enabling only necessary services, protocols, daemons, etc., as required for the function of the system * Implementing additional security features for any required services, protocols or daemons that are considered to be insecure * Configuring system security parameters to prevent misuse * Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers |  | | | | | |
| **2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)  **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.1.a** Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server. | **Identify the sample** of system components observed. |  | | | | | |
| *For each item in the sample*, **describe how** system configurations were inspected to verify that only one primary function per server is implemented. |  | | | | | |
| **2.2.1.b** If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device. | **Indicate** **whether** virtualization technologies are used. **(yes/no)** |  | | | | | |
| *If “no,”* **describe how** systems were observed to verify that no virtualization technologies are used. |  | | | | | |
| *If “yes”:* | | | | | | |
| **Identify** **the functions** for which virtualization technologies are used. |  | | | | | |
| **Identify the sample** of virtual system components or devices observed. |  | | | | | |
| *For each virtual system component and device in the sample*, **describe how** the system configurations were inspected to verify that only one primary function is implemented per virtual system component or device. |  | | | | | |
| **2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled. | **Identify the sample** of system components selected. |  | | | | | |
| *For each item in the sample*, **describe how** the enabled system services, daemons, and protocols were inspected to verify that only necessary services or protocols are enabled. |  | | | | | |
| **2.2.2.b** Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards. | *For each item in the sample of system components from 2.2.2.a,* **indicate whether** any insecure services, daemons, or protocols are enabled. **(yes/no)**  *If “no,” mark the remainder of 2.2.2.b and 2.2.3 as “Not Applicable.”* |  | | | | | |
| *If “yes,”* **identify responsible personnel** interviewed who confirm that a documented business justification was present for each insecure service, daemon, or protocol |  | | | | | |
| **2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.  ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 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 30th June, 2016.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.3.a** Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. | *If “yes” at 2.2.2.b, perform the following:* | | | | | | |
| **Identify** **configuration settings** inspected. |  | | | | | |
| **Describe how** configuration settings were inspected to verify that security features for all insecure services, daemons, or protocols are: | | | | | | |
| * Documented |  | | | | | |
| * Implemented |  | | | | | |
| **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 that 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. | **Indicate whether** the assessed entity includes POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS – for which the entity asserts are not susceptible to any known exploits for those protocols. **(yes/no)**  *If ‘no,’ mark the remainder of 2.2.3.b as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **identify the document(s)** examined to verifythat the entity maintains documentation that verifies the devices are not susceptible to any known exploits for SSL/early TLS. |  | | | | | |
| **2.2.3.c** *For all other environments using SSL and/or early TLS:*  Review the documented Risk Mitigation and Migration Plan to verify it includes:   * Description of usage, including; what data is 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 in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * 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 30th June 2016. | **Indicate whether** the assessed entity includes any other environments using SSL and/or early TLS **(yes/no)**  *If ‘no,’ mark the remainder of 2.2.3.c as ‘not applicable.’* |  | | | | | |
| If ‘yes,’ **identify the Risk Mitigation and Migration Plan document(s)** examined to verify that it includes:   * Description of usage, including; what data is 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 in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * 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 30th June 2016. |  | | | | | |
| **2.2.4** Configure system security parameters to prevent misuse. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.4.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components. | **Identify the system administrators and/or security managers** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed to verify that they have knowledge of common security parameter settings for system components. |  | | | | | |
| **2.2.4.b** Examine the system configuration standards to verify that common security parameter settings are included. | **Identify** **the system configuration standards** examined to verify that common security parameter settings are included. |  | | | | | |
| **2.2.4.c** Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards. | **Identify the sample** of system components selected. |  | | | | | |
| *For each item in the sample*, **describe how** the common security parameters were inspected to verify that they are set appropriately and in accordance with the configuration standards. |  | | | | | |
| **2.2.5** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.5.a** Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. | **Identify the sample** of system components selected. |  | | | | | |
| *For each item in the sample*, **describe how** the configurations were inspected to verify that all unnecessary functionality is removed. |  | | | | | |
| **2.2.5.b**. Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration. | **Describe how** the security parameters were examined with relevant documentation to verify that enabled functions are: | | | | | | |
| * Documented |  | | | | | |
| * Support secure configuration |  | | | | | |
| **2.2.5.c**. Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components. | **Identify** **documentation** examined for this testing procedure. |  | | | | | |
| **Describe how** the security parameters were examined with relevant documentation to verify that only documented functionality is present on the sampled system components from 2.2.5.a. |  | | | | | |
| **2.3** Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.  ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 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 30th June, 2016.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.3** Select a sample of system components and verify that non-console administrative access is encrypted by performing the following: | **Identify the sample** of system components selected for 2.3.a-2.3.d to verify that non-console administrative access is encrypted |  | | | | | |
| **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. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** the administrator log on for each system was observed to verify that a strong encryption method is invoked before the administrator’s password is requested. |  | | | | | |
| **Describe how** system configurations for each system were examined to verify that a strong encryption method is invoked before the administrator’s password is requested. |  | | | | | |
| **Identify** **the strong encryption method** used for non-console administrative access. |  | | | | | |
| **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. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** services on systems were reviewed to determine that Telnet and other insecure remote-login commands are not available for non-console access. |  | | | | | |
| **Describe how** parameter files on systems were reviewed 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. | *For each item in the sample from 2.3:* | | | | | | |
| **Describe how** the administrator log on to each system was observed to verify that administrator access to any web-based management interfaces was encrypted with strong cryptography. |  | | | | | |
| **Identify** **the strong encryption method** used for any web-based management interfaces. |  | | | | | |
| **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. | **Identify** **the vendor documentation** examined to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  | | | | | |
| **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 that 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. | **Indicate whether** the assessed entity includes POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS – for which the entity asserts are not susceptible to any known exploits for those protocols. **(yes/no)**  *If ‘no,’ mark the remainder of 2.3.e as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **identify the document(s)** examined to verifythat the entity maintains documentation that verifies the devices are not susceptible to any known exploits for SSL/early TLS. |  | | | | | |
| **2.3.f** *For all other environments using SSL and/or early TLS:*  Review the documented Risk Mitigation and Migration Plan to verify it includes:   * Description of usage, including; what data is 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 in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * 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 30th June 2016. | **Indicate whether** the assessed entity includes any other environments using SSL and/or early TLS **(yes/no)**  *If ‘no,’ mark the remainder of 2.3.f as ‘not applicable.’* |  | | | | | |
| *If ‘yes,’* **identify the Risk Mitigation and Migration Plan document(s)** examined to verify that it includes:   * Description of usage, including; what data is 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 in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * 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 30th June 2016. |  | | | | | |
| **2.4** Maintain an inventory of system components that are in scope for PCI DSS. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.4.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. | **Describe how** the system inventory was examined to verify that a list of hardware and software components is: | | | | | | |
| * Maintained |  | | | | | |
| * Includes a description of function/use for each |  | | | | | |
| **2.4.b** Interview personnel to verify the documented inventory is kept current. | **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that the documented inventory is kept current. |  | | | | | |
| **2.5** Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for managing vendor defaults and other security parameters are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for managing vendor defaults and other security parameters are:   * In use * Known to all affected parties |  | | | | | |
| **2.6** Shared hosting providers must protect each entity’s hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.6** Perform testing procedures **A.1.1** through **A.1.4** detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities’ (merchants and service providers) hosted environment and data. | **Indicate** **whether** the assessed entity is a shared hosting provider. **(yes/no)** |  | | | | | |
| *If “yes,”* **provide the name of the assessor** who attests that Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers has been completed. |  | | | | | |

## Protect Stored Cardholder Data

### Requirement 3: Protect stored cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | | **N/A** | **Not Tested** | **Not in Place** | |
| **3.1** Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes that include at least the following for all CHD storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. * Specific retention requirements for cardholder data * Processes for secure deletion of data when no longer needed. * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.1.a** Examine the data-retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. * Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). * Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. | **Identify the data-retention and disposal documentation** examined to verify policies, procedures, and processes define the following for all cardholder data (CHD) storage:   * Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements for data retention. * Specific requirements for retention of cardholder data. * Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons. * A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. |  | | | | | | | |
| **3.1.b** Interview personnel to verify that:   * All locations of stored cardholder data are included in the data-retention and disposal processes. * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. * The quarterly automatic or manual process is performed for all locations of cardholder data. | **Identify the personnel** interviewed who confirm that:   * All locations of stored cardholder data are included in the data-retention and disposal processes. * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. * The quarterly automatic or manual process is performed for all locations of cardholder data. |  | | | | | | | |
| For the interview, **summarize the relevant details** discussed that verify the following: | | | | | | | | |
| * All locations of stored cardholder data are included in the data-retention and disposal process. |  | | | | | | | |
| * Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. |  | | | | | | | |
| * The quarterly automatic or manual process is performed for all locations of cardholder data. |  | | | | | | | |
| **Describe** the quarterly process in place to identify and securely delete stored cardholder data, including whether it is an automatic or manual process. |  | | | | | | | |
| **3.1.c** For a sample of system components that store cardholder data:   * Examine files and system records to verify that the data stored does not exceed the requirements defined in the data-retention policy. * Observe the deletion mechanism to verify data is deleted securely. | **Identify the sample** of system components selected. |  | | | | | | | |
| *For each item in the sample*, **describe how** files and system records were examined to verify that the data stored does not exceed the requirements defined in the data-retention policy. |  | | | | | | | |
| **Describe how** the deletion mechanism was observed to verify data is deleted securely. |  | | | | | | | |
| **3.2** Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.  It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:   * There is a business justification, and * The data is stored securely.   Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data. | **Indicate whether** the assessed entity is an issuer or supports issuing service. **(yes/no)** |  | | | | | | | |
| *If “yes,” complete the responses for 3.2.a and 3.2.b and mark 3.2.c and 3.2.d as “Not Applicable.”*  *If “no,” mark the remainder of 3.2.a and 3.2.b as “Not Applicable” and proceed to 3.2.c and 3.2.d.* | | | | | | | | |
| **Identify** **the documentation** reviewed to verify there is a documented business justification for the storage of sensitive authentication data. |  | | | | | | | |
| **Identify** **the interviewed personnel** who confirm there is a documented business justification for the storage of sensitive authentication data. |  | | | | | | | |
| For the interview, **summarize the relevant details** of the business justification described. |  | | | | | | | |
| **3.2.b** For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured. | *If “yes” at 3.2.a,* | | | | | | | | |
| **Identify** **data stores** examined. |  | | | | | | | |
| **Identify the system configurations** examined. |  | | | | | | | |
| **Describe how** the data stores and system configurations were examined to verify that the sensitive authentication data is secured. |  | | | | | | | |
| **3.2.c** For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization. | **Indicate whether** sensitive authentication data is received. **(yes/no)** |  | | | | | | | |
| *If “yes,” complete 3.2.c and 3.2.d.*  *If “no,” mark the remainder of 3.2.c and 3.2.d as “Not Applicable” and proceed to 3.2.1.* | | | | | | | | |
| **Identify** **the document(s)** reviewed to verify that it defines that data is not retained after authorization. |  | | | | | | | |
| **Describe how** system configurations were examined to verify the data is not retained after authorization. |  | | | | | | | |
| **3.2.d** For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable. | **Identify** **the document(s)** reviewed to verify that it defines processes for securely deleting the data to verify that the data is unrecoverable. |  | | | | | | | |
| **Describe how** the processes for securely deleting the data were examined to verify that the data is unrecoverable. |  | | | | | | | |
| **3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.  **Note:** In the normal course of business, the following data elements from the magnetic stripe may need to be retained:   * The cardholder’s name * Primary account number (PAN) * Expiration date * Service code   To minimize risk, store only these data elements as needed for business. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | **Identify the sample** of system components selected for 3.2.1-3.2.3. |  | | | | | | | |
| *For each data source type below from the sample of system of components examined,* **summarize the specific examples of each data source type observed** to verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | | | |
| * Incoming transaction data |  | | | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | | | |
| * History files |  | | | | | | | |
| * Trace files |  | | | | | | | |
| * Database schemas |  | | | | | | | |
| * Database contents |  | | | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | | | |
| **3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | *For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed** to verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. If that type of data source is not present, indicate that in the space. | | | | | | | | |
| * Incoming transaction data |  | | | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | | | |
| * History files |  | | | | | | | |
| * Trace files |  | | | | | | | |
| * Database schemas |  | | | | | | | |
| * Database contents |  | | | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | | | |
| **3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents | *For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed**. If that type of data source is not present, indicate that in the space. | | | | | | | | |
| * Incoming transaction data |  | | | | | | | |
| * All logs (for example, transaction, history, debugging error) |  | | | | | | | |
| * History files |  | | | | | | | |
| * Trace files |  | | | | | | | |
| * Database schemas |  | | | | | | | |
| * Database contents |  | | | | | | | |
| * If applicable, **any other output observed** to be generated |  | | | | | | | |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.  **Note:** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **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 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 the full PAN. * All other roles not specifically authorized to see the full PAN must only see masked PANs. | **Identify the document(s)** reviewed to verify that written policies and procedures for masking the displays of PANs include the following:   * A list of roles that need access to displays of 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 the full PAN. * All other roles not specifically authorized to see the full PAN must only see masked PANs. |  | | | | | | | |
| **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. | **Describe how** system configurations were examined to verify that: | | | | | | | | |
| * Full PAN is only displayed for users/roles with a documented business need. |  | | | | | | | |
| * 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 full PAN. | **Describe how** displays of PAN were examined to verify that: | | | | | | | | |
| * PANs are masked when displaying cardholder data. |  | | | | | | | |
| * Only those with a legitimate business need are able to see full PAN. |  | | | | | | | |
| **3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:   * One-way hashes based on strong cryptography, (hash must be of the entire PAN). * Truncation (hashing cannot be used to replace the truncated segment of PAN). * Index tokens and pads (pads must be securely stored). * Strong cryptography with associated key-management processes and procedures.   **Note:** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity’s environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.4.a** Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures | **Identify** **the documentation** examined about the system used to protect the PAN. |  | | | | | | | |
| **Briefly describe** the documented methods—including the vendor, type of system/process, and then encryption algorithms (if applicable)— used to protect the PAN. |  | | | | | | | |
| **Identify** which of the following methods is used to render the PAN unreadable:   * One-way hashes based on strong cryptography * Truncation * Index token and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  | | | | | | | |
| **3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). | **Identify** **the sample** of data repositories selected. |  | | | | | | | |
| **Identify** **the tables or files** examined for each item in the sample of data repositories. |  | | | | | | | |
| *For each item in the sample*, **describe how** the table or file was examined to verify the PAN is rendered unreadable. |  | | | | | | | |
| **3.4.c** Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable. | **Identify the sample** of removable media selected. |  | | | | | | | |
| *For each item in the sample*, **describe how** the sample of removable media was examined to confirm that the PAN is rendered unreadable. |  | | | | | | | |
| **3.4.d** Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs. | **Identify the sample** of audit logs selected. |  | | | | | | | |
| *For each item in the sample,* **describe how** the sample of audit logs was examined to confirm that the PAN is rendered unreadable or removed from the logs. |  | | | | | | | |
| **3.4.e** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | **Identify whether** hashed and truncated versions of the same PAN are present in the environment **(yes/no)**  *If ‘no,’* mark 3.4.e as ‘not applicable’ and proceed to 3.4.1. |  | | | | | | | |
| *If ‘yes,’* **describe** the implemented controls examined to verify that the hashed and truncated versions cannot be correlated to reconstruct the original 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. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **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). | **Indicate whether** disk encryption is used. **(yes/no)** |  | | | | | | | |
| *If “yes,” complete the remainder of 3.4.1.a, 3.4.1.b, and 3.4.1.c.*  *If “no,” mark the remainder of 3.4.1.a, 3.4.1.b and 3.4.1.c as “Not Applicable.’* | | | | | | | | |
| **Describe** the disk encryption mechanism(s) in use. |  | | | | | | | |
| *For each disk encryption mechanism in use*, **describe how** the configuration was inspected and the authentication process observed to verify that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  | | | | | | | |
| **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). | **Describe how** processes were observed to verify that cryptographic keys are stored securely. |  | | | | | | | |
| **Identify the personnel** interviewed who confirm that cryptographic keys are stored securely. |  | | | | | | | |
| **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. | **Identify** **the configurations** examined. |  | | | | | | | |
| **Describe how** the configurations were examined and the processes observed to verify that cardholder data on removable media is encrypted wherever stored. |  | | | | | | | |
| **3.5** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:  **Note:** This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.5** Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * 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. * Keys are stored securely in the fewest possible locations and forms. | **Identify** **the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * 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. * Keys are stored securely in the fewest possible locations and forms. |  | | | | | | | |
| **3.5.1** Restrict access to cryptographic keys to the fewest number of custodians necessary. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.5.1** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary. | **Identify** **user access lists** examined. |  | | | | | | | |
| **Describe how** user access lists were examined to verify that access to keys is restricted to the fewest number of custodians necessary. |  | | | | | | | |
| **3.5.2** Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:   * Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. * Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). * As at least two full-length key components or key shares, in accordance with an industry-accepted method.   **Note:** It is not required that public keys be stored in one of these forms. | | | ☐ | ☐ | | ☐ | ☐ | | ☐ |
| **3.5.2.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. | **Identify** **the documented procedures** examined 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. |  | | | | | | | |
| **3.5.2.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. | **Provide the name** **of the assessor** who attests that all locations where keys are stored were identified. |  | | | | | | | |
| **Describe how** system configurations and key storage locations were examined 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. |  | | | | | | | |
| **3.5.2.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. | **Describe how** system configurations and key storage locations were examined to verify that, wherever key-encrypting keys are used: | | | | | | | | |
| * 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. |  | | | | | | | |
| **3.5.3** Store cryptographic keys in the fewest possible locations. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.5.3** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations. | **Describe how** key storage locations were examined and processes were observed to verify that keys are stored in the fewest possible locations. |  | | | | | | | |
| **3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:  **Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.a *Additional Procedure for service provider assessments only***: If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. | **Indicate whether** the assessed entity is a service provider that shares keys with their customers for transmission or storage of cardholder data. **(yes/no)** |  | | | | | | | |
| *If “yes,”* **Identify** **the document** that the service provider provides to their customers examined to verify that it includes guidance on how to securely transmit, store and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. |  | | | | | | | |
| **3.6.b** Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following: | | | | | | | | | |
| **3.6.1** Generation of strong cryptographic keys. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.1.a** Verify that key-management procedures specify how to generate strong keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to generate strong keys. |  | | | | | | | |
| **3.6.1.b** Observe the method for generating keys to verify that strong keys are generated. | **Describe how** the method for generating keys was observed to verify that strong keys are generated. |  | | | | | | | |
| **3.6.2** Secure cryptographic key distribution. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.2.a** Verify that key-management procedures specify how to securely distribute keys. | **Identify** **the documented key-management procedures** examined to verify procedures specify how to securely distribute keys. |  | | | | | | | |
| **3.6.2.b** Observe the method for distributing keys to verify that keys are distributed securely. | **Describe how** the method for distributing keys was observed to verify that keys are distributed securely. |  | | | | | | | |
| **3.6.3** Secure cryptographic key storage. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.3.a** Verify that key-management procedures specify how to securely store keys. | **Identify** **the documented key-management procedures examined** to verify procedures specify how to securely store keys. |  | | | | | | | |
| **3.6.3.b** Observe the method for storing keys to verify that keys are stored securely. | **Describe how** the method for storing keys was observed to verify that keys are stored securely. |  | | | | | | | |
| **3.6.4** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.6.4.a** Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). | **Identify** **the document** that defines:   * Key cryptoperiod(s) for each key type in use * A process for key changes at the end of the defined cryptoperiod(s) |  | | | | | | | |
| **3.6.4.b** Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s). | **Identify** **personnel interviewed** for this testing procedure who confirm that keys are changed at the end of the defined cryptoperiod(s). |  | | | | | | | |
| **3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.  **Note:** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **3.6.5.a** Verify that key-management procedures specify processes for the following:   * The retirement or replacement of keys when the integrity of the key has been weakened. * The replacement of known or suspected compromised keys. * Any keys retained after retiring or replacing are not used for encryption operations. | **Identify** **the key-management document** examined to verify that key-management processes specify the following:   * The retirement or replacement of keys when the integrity of the key has been weakened. * The replacement of known or suspected compromised keys. * Any keys retained after retiring or replacing are not used for encryption operations. |  | | | | | | | |
| **3.6.5.b** Interview personnel to verify the following processes are implemented:   * Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. * Keys are replaced if known or suspected to be compromised. * Any keys retained after retiring or replacing are not used for encryption operations. | **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** that verify the following processes are implemented: | | | | | | | | |
| * Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. |  | | | | | | | |
| * Keys are replaced if known or suspected to be compromised. |  | | | | | | | |
| * Any keys retained after retiring or replacing are not used for encryption operations. |  | | | | | | | |
| **3.6.6** If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.  **Note:** Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **3.6.6.a** Verify that manual clear-text key-management procedures specify processes for the use of the following:   * Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND * Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another. | **Indicate** **whether** manual clear-text cryptographic key-management operations are used. **(yes/no)** |  | | | | | | | |
| *If “no,” mark the remainder of 3.6.6.a and 3.6.6.b as “Not Applicable.”*  *If “yes,” complete 3.6.6.a and 3.6.6.b.* | | | | | | | | |
| **Identify the document** examined to verify that manual clear-text key-management procedures define processes for the use of the following:   * Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND * Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials of another. |  | | | | | | | |
| **3.6.6 b** Interview personnel and/or observe processes to verify that manual clear-text keys are managed with:   * Split knowledge, AND * Dual control | **Identify** **the personnel** interviewed for this testing procedure, if applicable. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed and/or describe how** processeswere observed to verify the following processes are implemented: | | | | | | | | |
| * Split knowledge |  | | | | | | | |
| * Dual Control |  | | | | | | | |
| **3.6.7** Prevention of unauthorized substitution of cryptographic keys. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **3.6.7.a** Verify that key-management procedures specify processes to prevent unauthorized substitution of keys. | **Identify** **the document** examined to verify that key-management procedures specify processes to prevent unauthorized substitution of keys. |  | | | | | | | |
| **3.6.7.b** Interview personnel and/or observe process to verify that unauthorized substitution of keys is prevented. | **Identify** **the personnel** interviewed for this testing procedure, if applicable. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** **and/or describe how** processes were observed to verify that unauthorized substitution of keys is prevented. |  | | | | | | | |
| **3.6.8** Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. | | | ☐ | ☐ | ☐ | | ☐ | ☐ | |
| **3.6.8.a** Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. | **Identify** **the document** examined to verify that key-management procedures specify processes for key custodians to acknowledge that they understand and accept their key-custodian responsibilities. |  | | | | | | | |
| **3.6.8.b** Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities. | **Describe how** key custodian acknowledgements or other evidence were observed to verify that key custodians have acknowledged that they understand and accept their key-custodian responsibilities. |  | | | | | | | |
| **3.7** Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **3.7** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are:   * Documented, * In use, and * Known to all affected parties | **Identify** **the document** reviewed to verify that security policies and operational procedures for protecting stored cardholder data are documented. |  | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for protecting stored cardholder data are:   * In use * Known to all affected parties |  | | | | | | | |

### Requirement 4: Encrypt transmission of cardholder data across open, public networks

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **4.1** Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:   * Only trusted keys and certificates are accepted. * The protocol in use only supports secure versions or configurations. * The encryption strength is appropriate for the encryption methodology in use.   ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 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 30th June, 2016.*  *Examples of open, public networks include but are not limited to:*   * *The Internet* * *Wireless technologies, including 802.11 and Bluetooth* * *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* * *General Packet Radio Service (GPRS)* * *Satellite communications* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **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. | **Identify** all locations where cardholder data is transmitted or received over open, public networks. |  | | | | | |
| **Identify** **the documented standards** examined. |  | | | | | |
| **Describe how** the documented standards were examined and compared to system configurations to verify the use of: | | | | | | |
| * Security protocols observed in use |  | | | | | |
| * 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. | **Identify the document** reviewed to verify that 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. |  | | | | | |
| **4.1.c** Select and observe a sample of inbound and outbound transmissions as they occur to verify that all cardholder data is encrypted with strong cryptography during transit. | **Describe** **the sample** of inbound and outbound transmissions observed as they occurred. |  | | | | | |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all cardholder data is encrypted with strong cryptography during transit. |  | | | | | |
| **4.1.d** Examine keys and certificates to verify that only trusted keys and/or certificates are accepted. | *For all instances where cardholder data is transmitted or received over open, public networks:* | | | | | | |
| **Describe the mechanisms** used to ensure that only trusted keys and/or certificates are accepted. |  | | | | | |
| **Describe how** the mechanisms were observed to accept only trusted keys and/or certificates. |  | | | | | |
| **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. | *For all instances where cardholder data Is transmitted or received over open, public networks,* **describe how** system configurations were observed to verify that the protocol is implemented: | | | | | | |
| * To use only secure configurations. |  | | | | | |
| * 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.) | *For each encryption methodology in use,* | | | | | | |
| **Identify** vendor recommendations/best practices for encryption strength. |  | | | | | |
| **Identify** the encryption strength observed to be implemented. |  | | | | | |
| **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.* | **Indicate whether** TLS is implemented to encrypt cardholder data over open, public networks in the CDE. **(yes/no)** |  | | | | | |
| *If “yes,” for all instances where TLS is used to encrypt cardholder data over open, public networks,* ***describe how*** *system configurations were examined to verify that TLS is enabled whenever cardholder data is transmitted or received, as follows:* | | | | | | |
| * HTTPS appears as part of the browser URL. |  | | | | | |
| * Cardholder data is only requested if HTTPS appears as part of the URL. |  | | | | | |
| **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 that 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. | **Indicate whether** the assessed entity includes POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS – for which the entity asserts are not susceptible to any known exploits for those protocols. **(yes/no)**  *If ‘no,’ mark the remainder of 4.1.h as ‘not applicable.’* |  | | | | | |
| *If ‘yes*,’ **identify the document(s)** examined to verifythat the entity maintains documentation that verifies the devices are not susceptible to any known exploits for SSL/early TLS. |  | | | | | |
| **4.1.i** *For all other environments using SSL and/or early TLS:*  Review the documented Risk Mitigation and Migration Plan to verify it includes:   * Description of usage, including; what data is 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 in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * 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 30th June 2016. | **Indicate whether** the assessed entity includes any other environments using SSL and/or early TLS **(yes/no)**  *If ‘no,’ mark the remainder of 4.1.i as ‘not applicable.’* |  | | | | | |
| If ‘yes,’ **identify the Risk Mitigation and Migration Plan document(s)** examined to verify that it includes:   * Description of usage, including; what data is 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 in place; * Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; * 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 30th June 2016. |  | | | | | |
| **4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.  **Note:** The use of WEP as a security control is prohibited. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.1.1** Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified:   * Industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. * Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission. | **Identify** all wireless networks transmitting cardholder data or connected to the cardholder data environment. |  | | | | | |
| **Identify the documented standards** examined to verify processes define the following for all wireless networks identified:   * Industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. * Weak encryption is not used as a security control for authentication or transmission. |  | | | | | |
| **Describe how** documented standards were examined and compared to system configuration settings to verify the following for all wireless networks identified: | | | | | | |
| * Industry best practices are used to implement strong encryption for authentication and transmission. |  | | | | | |
| * Weak encryption is not used as a security control for authentication or transmission. |  | | | | | |
| **4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.2.a** If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. | **Indicate** **whether** end-user messaging technologies are used to send cardholder data. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 4.2.a as “Not Applicable” and proceed to 4.2.b.*  *If “yes,” complete the following:* | | | | | | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | | | | | |
| **Describe how** the sample of outbound transmissions observed as they occurred to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | | | | | |
| **4.2.b** Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies. | *If “yes” at 4.2.a:* |  | | | | | |
| **Identify** **the policy document** stating that unprotected PANs must not be sent via end-user messaging technologies. |  | | | | | |
| *If “no” at 4.2.a:* | | | | | | |
| **Identify** **the policy document** that explicitly prohibits PAN from being sent via end-user messaging technologies under any circumstances. |  | | | | | |
| **4.3** Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.3** Examine documentation and interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for encrypting transmissions of cardholder data are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for encrypting transmissions of cardholder data are:   * In use * Known to all affected parties |  | | | | | |

## Maintain a Vulnerability Management Program

### Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | | | **N/A** | **Not Tested** | **Not in Place** |
| **5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). | | | ☐ | ☐ | | | ☐ | ☐ | ☐ |
| **5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | **Identify the sample** of system components selected (including all operating system types commonly affected by malicious software). |  | | | | | | | |
| *For each item in the sample*, **describe how** anti-virus software was observed to be deployed. |  | | | | | | | |
| **5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | | | ☐ | ☐ | | ☐ | | ☐ | ☐ |
| 5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software.   *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).* | **Identify** **the vendor documentation** reviewed to verify that anti-virus programs:   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  | | | | | | | |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | | | | | | | | |
| * Detect all known types of malicious software, |  | | | | | | | |
| * Remove all known types of malicious software, and |  | | | | | | | |
| * Protect against all known types of malicious software. |  | | | | | | | |
| **5.1.2** For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. | | | ☐ | ☐ | ☐ | | | ☐ | ☐ |
| **5.1.2** Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software. | **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** **and/or describe how processes** were observed to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, and that such systems continue to not require anti-virus software. |  | | | | | | | |
| **5.2** Ensure that all anti-virus mechanisms are maintained as follows:   * Are kept current. * Perform periodic scans. * Generate audit logs which are retained per PCI DSS Requirement 10.7. | | | ☐ | ☐ | | | ☐ | ☐ | ☐ |
| **5.2.a** Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up-to-date. | **Identify** **the documented policies and procedures** examined to verify that anti-virus software and definitions are required to be kept up to date. |  | | | | | | | |
| **5.2.b** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are:   * Configured to perform automatic updates, and * Configured to perform periodic scans. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are: | | | | | | | | |
| * Configured to perform automatic updates, and |  | | | | | | | |
| * Configured to perform periodic scans. |  | | | | | | | |
| **5.2.c** Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:   * The anti-virus software and definitions are current. * Periodic scans are performed. | **Identify the sample** of system components, including all operating system types commonly affected by malicious software, selected for this testing procedure. |  | | | | | | | |
| **Describe how** system components were examined to verify that: | | | | | | | | |
| * The anti-virus software and definitions are current. |  | | | | | | | |
| * Periodic scans are performed. |  | | | | | | | |
| **5.2.d** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:   * Anti-virus software log generation is enabled, and * Logs are retained in accordance with PCI DSS Requirement 10.7. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | | | |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, were examined to verify that: | | | | | | | | |
| * Anti-virus software log generation is enabled, and |  | | | | | | | |
| * Logs are retained in accordance with PCI DSS Requirement 10.7. |  | | | | | | | |
| **5.3** Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.  **Note:** Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active. | | | ☐ | ☐ | | | ☐ | ☐ | ☐ |
| **5.3.a** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running. | **Identify** **the sample** of system components selected. |  | | | | | | | |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, were examined to verify that the anti-virus software is actively running. |  | | | | | | | |
| **5.3.b** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users. | *For each item in the sample from 5.3.a,* **describe how** anti-virus configurations, including the master installation of the software, were examined to verify that the anti-virus software cannot be disabled or altered by users. |  | | | | | | | |
| **5.3.c** Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. | **Identify** **the responsible personnel** interviewed who confirm that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  | | | | | | | |
| **Describe how** the process was observed to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  | | | | | | | |
| **5.4** Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. | | | ☐ | ☐ | | | ☐ | ☐ | ☐ |
| **5.4** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for protecting systems against malware are documented. |  | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for protecting systems against malware are:   * In use * Known to all affected parties |  | | | | | | | |

### Requirement 6: Develop and maintain secure systems and applications

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | | **N/A** | **Not Tested** | **Not in Place** | |
| **6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.  **Note:** Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.  Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.1.a** Examine policies and procedures to verify that processes are defined for the following:   * To identify new security vulnerabilities. * To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. * To include using reputable outside sources for security vulnerability information. | **Identify** **the documented policies and procedures** examined to confirm that processes are defined:   * To identify new security vulnerabilities. * To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities. * To include using reputable outside sources for security vulnerability information. |  | | | | | | | |
| **6.1.b** Interview responsible personnel and observe processes to verify that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. | **Identify the responsible personnel** interviewed who confirm that:   * New security vulnerabilities are identified. * A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities. * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  | | | | | | | |
| **Describe** the processes observed to verify that: | | | | | | | | |
| * New security vulnerabilities are identified. |  | | | | | | | |
| * A risk ranking is assigned to vulnerabilities to include identification of all “high” risk and “critical” vulnerabilities. |  | | | | | | | |
| * Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  | | | | | | | |
| **Identify** the outside sources used. |  | | | | | | | |
| **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). | **Identify** **the documented policies and procedures** related to security-patch installation examined 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. |  | | | | | | | |
| **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). | **Identify** **the sample** of system components and related software selected for this testing procedure. |  | | | | | | | |
| **Identify** **the vendor security patch list** reviewed. |  | | | | | | | |
| *For each item in the sample,* **describe how** the list of security patches installed on each system was compared to the most recent vendor security-patch list to verify 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. |  | | | | | | | |
| **6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:   * In accordance with PCI DSS (for example, secure authentication and logging). * Based on industry standards and/or best practices. * Incorporate information security throughout the software development life cycle.   **Note**: this applies to all software developed internally as well as bespoke or custom software developed by a third party. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.3.a** Examine written software-development processes to verify that the processes are based on industry standards and/or best practices. | **Identify** **the document** that defines software development processes based on industry standards and/or best practices. |  | | | | | | | |
| **Identify** the industry standards and/or best practices used. |  | | | | | | | |
| **6.3.b** Examine written software development processes to verify that information security is included throughout the life cycle. | **Identify** **the documented software development processes** examined to verify that information security is included throughout the life cycle. |  | | | | | | | |
| **6.3.c** Examine written software development processes to verify that software applications are developed in accordance with PCI DSS. | **Identify** **the documented software development processes** examined to verify that software applications are developed in accordance with PCI DSS. |  | | | | | | | |
| **6.3.d** Interview software developers to verify that written software development processes are implemented. | **Identify** **the software developers** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that written software development processes are implemented. |  | | | | | | | |
| **6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.3.1** Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. | **Identify** **the documented software-development processes** examined to verify processes define that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  | | | | | | | |
| **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  | | | | | | | |
| **6.3.2** Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:   * Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines. * Appropriate corrections are implemented prior to release. * Code review results are reviewed and approved by management prior to release.   **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.  *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.* | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.3.2.a** Examine written software development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. | **Identify** **the documented software-development processes** examined to verify processes define that all custom application code changes must be reviewed (using either manual or automated processes) as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  | | | | | | | |
|  | **Identify** **the responsible personnel** interviewed for this testing procedure who confirm that all custom application code changes are reviewed as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  | | | | | | | |
| **Describe how** all custom application code changes must be reviewed, including whether processes are manual or automated. |  | | | | | | | |
| **6.3.2.b** Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above. | **Identify** **the sample** of recent custom application changes selected for this testing procedure. |  | | | | | | | |
| *For each item in the sample*, **describe how** code review processes were observed to verify custom application code is reviewed as follows: | | | | | | | | |
| * Code changes are reviewed by individuals other than the originating code author. |  | | | | | | | |
| * Code changes are reviewed by individuals who are knowledgeable in code-review techniques and secure coding practices. |  | | | | | | | |
| * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). |  | | | | | | | |
| * Appropriate corrections are implemented prior to release. |  | | | | | | | |
| * Code-review results are reviewed and approved by management prior to release. |  | | | | | | | |
| **6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following: | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4** Examine policies and procedures to verify the following are defined:   * Development/test environments are separate from production environments with access control in place to enforce separation. * A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. * Production data (live PANs) are not used for testing or development. * Test data and accounts are removed before a production system becomes active. * Change control procedures related to implementing security patches and software modifications are documented. | **Identify the documented policies and procedures** examined to verify that the following are defined:   * Development/test environments are separate from production environments with access control in place to enforce separation. * A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. * Production data (live PANs) are not used for testing or development. * Test data and accounts are removed before a production system becomes active. * Change-control procedures related to implementing security patches and software modifications are documented. |  | | | | | | | |
| **6.4.1** Separate development/test environments from production environments, and enforce the separation with access controls. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.1.a** Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s). | **Identify the network documentation** that illustrates that the development/test environments are separate from the production environment(s). |  | | | | | | | |
| **Describe how** network device configurations were examined to verify that the development/test environments are separate from the production environment(s). |  | | | | | | | |
| **6.4.1.b** Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s). | **Identify the access control settings** examined for this testing procedure. |  | | | | | | | |
| **Describe how** the access control settings were examined to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s). |  | | | | | | | |
| **6.4.2** Separation of duties between development/test and production environments. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.2** Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment. | **Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  | | | | | | | |
| **Identify the personnel assigned to production environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  | | | | | | | |
| **Describe how** processes were observed to verify that separation of duties is in place between development/test environments and the production environment. |  | | | | | | | |
| **6.4.3** Production data (live PANs) are not used for testing or development. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.3.a** Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development. | **Identify the personnel** interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development. |  | | | | | | | |
| **Describe how** testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing. |  | | | | | | | |
| **Describe how** testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development. |  | | | | | | | |
| **6.4.3.b** Examine a sample of test data to verify production data (live PANs) is not used for testing or development. | **Describe how** a sample of test data was examined to verify production data (live PANs) is not used for testing. |  | | | | | | | |
| **Describe how** a sample of test data was examined to verify production data (live PANs) is not used for development. |  | | | | | | | |
| **6.4.4** Removal of test data and accounts before production systems become active. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.4.a** Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active. | **Identify the personnel** interviewed who confirm that test data and accounts are removed before a production system becomes active. |  | | | | | | | |
| **Describe how** testing processes were observed to verify that test data is removed before a production system becomes active. |  | | | | | | | |
| **Describe how** testing processes were observed to verify that test accounts are removed before a production system becomes active. |  | | | | | | | |
| **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. | **Describe how** a sample of data from production systems recently installed or updated was examined to verify test data is removed before the system becomes active. |  | | | | | | | |
| **Describe how** a sample of accounts from production systems recently installed or updated was examined to verify test accounts are removed before the system becomes active. |  | | | | | | | |
| **6.4.5** Change control procedures for the implementation of security patches and software modifications must include the following: | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.5.a** Examine documented change-control procedures related to implementing security patches and software modifications and verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. | **Identify** **the documented change-control procedures** related to implementing security patches and software modification examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  | | | | | | | |
| **6.4.5.b** For a sample of system components, interview responsible personnel to determine recent changes/security patches. Trace those changes back to related change control documentation. For each change examined, perform the following: | **Identify** **the sample** of system components selected. |  | | | | | | | |
| **Identify the responsible personnel** interviewed to determine recent changes/security patches. |  | | | | | | | |
| *For each item in the sample,* **identify** **the sample** of changes and the related change control documentation selected for this testing procedure (through 6.4.5.4) |  | | | | | | | |
| **6.4.5.1** Documentation of impact. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change. | *For each change from 6.4.5.b*, **describe how** the changes were traced back to the identified related change control documentation to verify that documentation of impact is included in the change control documentation for each sampled change. |  | | | | | | | |
| **6.4.5.2** Documented change approval by authorized parties. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change. | *For each change from 6.4.5.b*, **describe how** the changes were traced back to the identified related change control documentation to verify that documented approval by authorized parties is present in the change control documentation for each sampled change. |  | | | | | | | |
| **6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. | *For each change from 6.4.5.b*, **describe how** the changes were traced back to the identified related change control documentation to verify that the change control documentation for each sampled change includes evidence that functionality testing is performed to verify that the change does not adversely impact the security of the system. |  | | | | | | | |
| **6.4.5.3.b** For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | | | |
| *For each item in the sample,* **identify** **the sample** of custom code changes and the related change control documentation selected for this testing procedure. |  | | | | | | | |
| **Describe how** the custom code changes were traced back to the identified related change control documentation to verify that the change control documentation for each sampled custom code change includes evidence that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. |  | | | | | | | |
| **6.4.5.4** Back-out procedures. | | | ☐ | ☐ | | ☐ | ☐ | | ☐ |
| **6.4.5.4** Verify that back-out procedures are prepared for each sampled change. | *For each change from 6.4.5.b*, **describe how** the changes were traced back to the identified related change control documentation to verify that back-out procedures are prepared for each sampled change and present in the change control documentation for each sampled change. |  | | | | | | | |
| **6.5** Address common coding vulnerabilities in software-development processes as follows:   * Traindevelopers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. * Develop applications based on secure coding guidelines.   **Note:** The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, 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 training in secure coding techniques is required for developers, based on industry best practices and guidance. | **Identify** **the document** reviewed to verify that training in secure coding techniques is required for developers. |  | | | | | | | |
| **Identify** the industry best practices and guidance that training is based on. |  | | | | | | | |
| **6.5.b** Interview a sample of developers to verify that they are knowledgeable in secure coding techniques. | **Identify** **the developers** interviewed for this testing procedure. |  | | | | | | | |
| For the interview, **summarize the relevant details discussed** to verify that they are knowledgeable in secure coding techniques. |  | | | | | | | |
| **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. | **Identify the records** **of training** that were examined 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. |  | | | | | | | |
| **6.5.d.** Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: | **Identify** **the software-development policies and procedures** examined to verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: |  | | | | | | | |
| **Identify** **the responsible personnel** interviewed to verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: |  | | | | | | | |
| **Note:** Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external): | | | | | | | | | |
| **6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.1** Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include:   * Validating input to verify user data cannot modify meaning of commands and queries. * Utilizing parameterized queries. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that injection flaws are addressed by coding techniques that include: | | | | | | | | |
| * Validating input to verify user data cannot modify meaning of commands and queries. |  | | | | | | | |
| * Utilizing parameterized queries. |  | | | | | | | |
| **6.5.2** Buffer overflow. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.2** Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include:   * Validating buffer boundaries. * Truncating input strings. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that buffer overflows are addressed by coding techniques that include: | | | | | | | | |
| * Validating buffer boundaries. |  | | | | | | | |
| * Truncating input strings. |  | | | | | | | |
| **6.5.3** Insecure cryptographic storage. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.3** Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that:   * Prevent cryptographic flaws. * Use strong cryptographic algorithms and keys. | *For the interviews at 6.5.d,* **summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that insecure cryptographic storage is addressed by coding techniques that: | | | | | | | | |
| * Prevent cryptographic flaws. |  | | | | | | | |
| * Use strong cryptographic algorithms and keys. |  | | | | | | | |
| **6.5.4** Insecure communications. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.4** Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications. | *For the interviews at 6.5.d,* **summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that insecure communications are addressed by coding techniques that properly: | | | | | | | | |
| * Authenticate all sensitive communications. |  | | | | | | | |
| * Encrypt all sensitive communications. |  | | | | | | | |
| **6.5.5** Improper error handling. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.5** Examine-software development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages(for example, by returning generic rather than specific error details). | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that improper error handling is addressed by coding techniques that do not leak information via error messages. |  | | | | | | | |
| **6.5.6** All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.6** Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any “high risk” vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1. | *For the interviews at 6.5.d,* **summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that applications are not vulnerable to “High” vulnerabilities, as identified in PCI DSS Requirement 6.1. |  | | | | | | | |
| **Note:** Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external): | | | | | | | | | |
| **Indicate** **whether** web applications and application interfaces are present. **(yes/no)**  *If “no,”* mark the below 6.5.7-6.5.10 as “Not Applicable.”  *If “yes,”* ***complete the following:*** | |  | | | | | | | |
| **6.5.7** Cross-site scripting (XSS). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.7** Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include:   * Validating all parameters before inclusion. * Utilizing context-sensitive escaping. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that cross-site scripting (XSS) is addressed by coding techniques that include: | | | | | | | | |
| * Validating all parameters before inclusion. |  | | | | | | | |
| * Utilizing context-sensitive escaping. |  | | | | | | | |
| **6.5.8** Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.8** Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that include:   * Proper authentication of users. * Sanitizing input. * Not exposing internal object references to users. * User interfaces that do not permit access to unauthorized functions. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that improper access control is addressed by coding techniques that include: | | | | | | | | |
| * Proper authentication of users. |  | | | | | | | |
| * Sanitizing input. |  | | | | | | | |
| * Not exposing internal object references to users. |  | | | | | | | |
| * User interfaces that do not permit access to unauthorized functions. |  | | | | | | | |
| **6.5.9** Cross-site request forgery (CSRF). | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.9** Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. | *For the interviews at 6.5.d***, summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. |  | | | | | | | |
| **6.5.10** Broken authentication and session management**.**  **Note:** Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.5.10** Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include:   * Flagging session tokens (for example cookies) as “secure.” * Not exposing session IDs in the URL. * Incorporating appropriate time-outs and rotation of session IDs after a successful login. | **Indicate whether** this ROC is being completed prior to June 30, 2015**. (yes/no)** |  | | | | | | | |
| *If “yes” AND the assessed entity does not have this in place ahead of the requirement’s effective date, mark the remainder of 6.5.10 as “Not Applicable.”*  *If “no” OR if the assessed entity has this in place ahead of the requirement’s effective date, complete the following:* | | | | | | | | |
| *For the interviews at 6.5.d,* **summarize the relevant interview details** that confirm processes are in place, consistent with the software development documentation at 6.5.d, to ensure that broken authentication and session management are addressed via coding techniques that protect credentials and session IDs, including: | | | | | | | | |
| * Flagging session tokens (for example cookies) as “secure.” |  | | | | | | | |
| * Not exposing session IDs in the URL. |  | | | | | | | |
| * Implementing appropriate time-outs and rotation of session IDs after a successful login |  | | | | | | | |
| **6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:   * Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.   **Note:** This assessment is not the same as the vulnerability scans performed for Requirement 11.2.   * Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.6** For *public-facing* web applications, ensure that *either* one of the following methods is in place as follows:   * Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. * Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * Is generating audit logs. * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. | For each public-facing web application, **identify which** of the two methods are implemented:   * Web application vulnerability security assessments, AND/OR * Automated technical solution that detects and prevents web-based attacks, such as web application firewalls. |  | | | | | | | |
| *If application vulnerability security assessments are indicated above:* | | | | | | | | |
| **Describe the tools and/or methods** used (manual or automated, or a combination of both). |  | | | | | | | |
| **Identify the organization(s)** confirmed to specialize in application security that is performing the assessments. |  | | | | | | | |
| **Identify the documented processes** that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows:   * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected * That the application is re-evaluated after the corrections. |  | | | | | | | |
| **Identify the responsible personnel** interviewed who confirm that public-facing web applications are reviewed, as follows:   * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. |  | | | | | | | |
| **Identify the records of application security assessments** examined for this testing procedure. |  | | | | | | | |
| **Describe how** the records of application security assessments were examined to verify that public-facing web applications are reviewed as follows: | | | | | | | | |
| * At least annually. |  | | | | | | | |
| * After any changes. |  | | | | | | | |
| * By an organization that specialized in application security. |  | | | | | | | |
| * That at a minimum, all vulnerabilities in requirement 6.5 are included in the assessment. |  | | | | | | | |
| * That all vulnerabilities are corrected. |  | | | | | | | |
| * That the application is re-evaluated after the corrections. |  | | | | | | | |
| *If an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is indicated above:* | | | | | | | | |
| **Describe** the automated technical solution in use that detects and prevents web-based attacks. |  | | | | | | | |
| **Identify** the responsible personnel interviewed who confirm that the above automated technical solution in use to detect and prevent web-based attacks is in place as follows:   * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * Is generating audit logs. * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  | | | | | | | |
| **Identify the system configuration settings** examined for this testing procedure. |  | | | | | | | |
| **Describe how** the system configuration settings were examined to verify that the above automated technical solution is use to detect and prevent web-based attacks is in place as follows: | | | | | | | | |
| * Is situated in front of public-facing web applications to detect and prevent web-based attacks. |  | | | | | | | |
| * Is actively running and up-to-date as applicable. |  | | | | | | | |
| * Is generating audit logs. |  | | | | | | | |
| * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  | | | | | | | |
| **6.7** Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. | | | ☐ | ☐ | | ☐ | ☐ | ☐ | |
| **6.7** Examine documentation and interview personnel to verify that security policies and operational procedures for developing and maintaining secure systems and applications are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for developing and maintaining secure systems and applications are documented. |  | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for developing and maintaining secure systems and applications are:   * In use * Known to all affected parties |  | | | | | | | |

## Implement Strong Access Control Measures

### Requirement 7: Restrict access to cardholder data by business need to know

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.a** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function. * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  | | | | | |
| **7.1.1** Define access needs for each role, including:   * System components and data resources that each role needs to access for their job function. * Level of privilege required (for example, user, administrator, etc.) for accessing resources. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.1** Select a sample of roles and verify access needs for each role are defined and include:   * System components and data resources that each role needs to access for their job function. * Identification of privilege necessary for each role to perform their job function. | **Identify** **the selected sample** of roles for this testing procedure. |  | | | | | |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | | | | | | |
| * System components and data resources that each role needs to access for their job function. |  | | | | | |
| * Identification of privilege necessary for each role to perform their job function. |  | | | | | |
| **7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.2.a** Interview personnel responsible for assigning access to verify that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. | **Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| **7.1.2.b** Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are:   * Necessary for that individual’s job function. * Restricted to least privileges necessary to perform job responsibilities. | **Identify the sample** of user IDs ***with privileged access*** selected for this testing procedure. |  | | | | | |
| **Identify** **the responsible management personnel** interviewed to confirm that privileges assigned are:   * Necessary for that individual’s job function. * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each user ID in the selected sample are: | | | | | | |
| * Necessary for that individual’s job function. |  | | | | | |
| * Restricted to least privileges necessary to perform job responsibilities. |  | | | | | |
| **7.1.3** Assign access based on individual personnel’s job classification and function. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.3** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual’s job classification and function. | **Identify the sample** of user IDs examined for this testing procedure. |  | | | | | |
| **Identify** **the responsible management personnel** interviewed who confirm that privileges assigned are based on that individual’s job classification and function. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each user ID in the selected sample are based on an individual’s job classification and function. |  | | | | | |
| **7.1.4** Require documented approval by authorized parties specifying required privileges. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.4** Select a sample of user IDs and compare with documented approvals to verify that:   * Documented approval exists for the assigned privileges. * The approval was by authorized parties. * That specified privileges match the roles assigned to the individual. | **Identify the sample** of user IDs examined for this testing procedure. |  | | | | | |
| **Describe how** each item in the sample of user IDs was compared with documented approvals to verify that: | | | | | | |
| * Documented approval exists for the assigned privileges. |  | | | | | |
| * The approval was by authorized parties. |  | | | | | |
| * That specified privileges match the roles assigned to the individual. |  | | | | | |
| **7.2** Establish an access control system for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.  This access control system must include the following: | | | | | | | |
| **7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows: | | | | | | | |
| **7.2.1** Coverage of all system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.1** Confirm that access control systems are in place on all system components. | **Identify** **vendor documentation** examined. |  | | | | | |
| **Describe how** system settings were examined with the vendor documentation to verify that access control systems are in place on all system components. |  | | | | | |
| **7.2.2** Assignment of privileges to individuals based on job classification and function. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. | **Describe how** system settings were examined with the vendor documentation at 7.2.1 to verify that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. |  | | | | | |
| **7.2.3** Default “deny-all” setting. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.3** Confirm that the access control systems have a default “deny-all” setting. | **Describe how** system settings were examined with vendor documentation at 7.2.1 to verify that access control systems have a default “deny-all” setting. |  | | | | | |
| **7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.3** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for restricting access to cardholder data are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for restricting access to cardholder data are:   * In use * Known to all affected parties |  | | | | | |

### Requirement 8: Identify and authenticate access to system components

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.a** Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below at 8.1.1 through 8.1.8:   * Assign all users a unique ID before allowing them to access system components or cardholder data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: * Enabled only during the time period needed and disabled when not in use. * Monitored when in use. * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  | | | | | |
| **8.1.b** Verify that procedures are implemented for user identification management, by performing the following: | | | | | | | |
| **8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.1** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data. | **Identify** **the responsible administrative personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that all users are assigned a unique ID for access to system components or cardholder data. |  | | | | | |
| **8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.2** For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval. | **Identify** **the sample** of privileged user IDs selected for this testing procedure. |  | | | | | |
| **Identify** **the sample** of general user IDs selected for this testing procedure. |  | | | | | |
| **Describe how** observed system settings and the associated authorizations documented for the user IDs were compared to verify that each ID has been implemented with only the privileges specified on the documented approval: | | | | | | |
| * For the sample of privileged user IDs. |  | | | | | |
| * For the sample of general user IDs. |  | | | | | |
| **8.1.3** Immediately revoke access for any terminated users. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.3.a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. | **Identify** **the sample** of users terminated in the past six months selected. |  | | | | | |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  | | | | | |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  | | | | | |
| **8.1.3.b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. | *For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination. |  | | | | | |
| **Describe how** the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated. |  | | | | | |
| **8.1.4** Remove/disable inactive user accounts within 90 days. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled. | **Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled. |  | | | | | |
| **8.1.5** Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:   * Enabled only during the time period needed and disabled when not in use. * Monitored when in use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.5.a** Interview personnel and observe processes for managing accounts used by vendors to access, support, or maintain system components to verify that accounts used by vendors for remote access are:   * Disabled when not in use. * Enabled only when needed by the vendor, and disabled when not in use. | **Identify** **the personnel** interviewed who confirm that accounts used by vendors for remote access are:   * Disabled when not in use. * Enabled only when needed by the vendor, and disabled when not in use. |  | | | | | |
| **Describe how** processes for managing accounts used by vendors to access, support, or maintain system components were observed to verify that accounts used by vendors for remote access are: | | | | | | |
| * Disabled when not in use. |  | | | | | |
| * Enabled only when needed by the vendor, and disabled when not in use. |  | | | | | |
| **8.1.5.b** Interview personnel and observe processes to verify that vendor remote access accounts are monitored while being used. | **Identify** **the personnel** interviewed who confirm that accounts used by vendors for remote access are monitored while being used. |  | | | | | |
| **Describe how** processes for managing accounts used by vendors to access, support, or maintain system components were observed to verify that vendor remote access accounts are monitored while being used. |  | | | | | |
| **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.6.a** For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that authentication parameters are set to require that user accounts be locked after not more than six invalid logon attempts. |  | | | | | |
| **8.1.6.b** ***Additional procedure for service provider assessments only:*** Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  | | | | | |
| **Describe** the implemented processes that were observed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  | | | | | |
| **8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.7** For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. |  | | | | | |
| **8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.8** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. | **Identify** **the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that system/session idle time out features have been set to 15 minutes or less. |  | | | | | |
| **8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:   * Something you know, such as a password or passphrase. * Something you have, such as a token device or smart card. * Something you are, such as a biometric. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following:   * Examine documentation describing the authentication method(s) used. * For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s). | **Identify the document** describing the authentication method(s) used that was reviewed to verify that the methods require users to be authenticated using a unique ID and additional authentication for access to the cardholder data environment. |  | | | | | |
| **Describe** the authentication methods used (for example, a password or passphrase, a token device or smart card, a biometric, etc.) for each type of system component. |  | | | | | |
| *For each type of authentication method used and for each type of system component,***describe how** the authentication method was observed to be: | | | | | | |
| * Used for access to the cardholder data environment. |  | | | | | |
| * Functioning consistently with the documented authentication method(s). |  | | | | | |
| **8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.1.a** Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage. | **Identify** **the vendor documentation** reviewed for this testing procedure. |  | | | | | |
| **Identify the sample** of system components selected. |  | | | | | |
| *For each item in the sample,***describe how** system configuration settings were examined to verify that passwords are protected with strong cryptography during ***transmission***. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were examined to verify that passwords are protected with strong cryptography during ***storage***. |  | | | | | |
| **8.2.1.b** For a sample of system components, examine password files to verify that passwords are unreadable during storage. | *For each item in the sample at 8.2.1.a,* **describe how** password files were examined to verify that passwords are unreadable during storage. |  | | | | | |
| **8.2.1.c** For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission. | *For each item in the sample at 8.2.1.a,* **describe how** password files were examined to verify that passwords are unreadable during transmission. |  | | | | | |
| **8.2.1.d** ***Additional procedure for service provider assessments only:*** Observe password files to verify that non-consumer customer passwords are unreadable during storage. | *Additional procedure for service provider assessments only:**for each item in the sample at 8.2.1.a,* **describe how** password files were examined to verify that non-consumer customer passwords are unreadable during storage. |  | | | | | |
| **8.2.1.e *Additional procedure for service provider assessments only:*** Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission. | *Additional procedure for service provider assessments only:**for each item in the sample at 8.2.1.a,* **describe how** password files were examined to verify that non-consumer customer passwords are unreadable during transmission. |  | | | | | |
| **8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.2** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the authentication credential is modified. | **Identify the document** examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  | | | | | |
| **Describe** the non-face-to-face methods used for requesting password resets. |  | | | | | |
| **Describe how** security personnel were observed to verify that if a user requests a reset of an authentication credential by a non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  | | | | | |
| **8.2.3** Passwords/phrases must meet the following:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters.   Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.3.a** For a sample of system components, inspect system configuration settings to verify that user password 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. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that user password 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. |  | | | | | |
| **8.2.3.b** ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that non-consumer customer passwords 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. | *Additional procedure for service provider assessments only:***Identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer passwords are required to meet at least the following strength/complexity:   * A minimum length of at least seven characters. * Non-consumer user passwords are required to contain both numeric and alphabetic characters. |  | | | | | |
| **Describe how** internal processes were reviewed to verify that non-consumer customer passwords are required to meet at least the following strength/complexity: | | | | | | |
| * A minimum length of at least seven characters. |  | | | | | |
| * Non-consumer customer passwords are required to contain both numeric and alphabetic characters. |  | | | | | |
| **8.2.4** Change user passwords/passphrases at least once every 90 days. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least once every 90 days. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that user password parameters are set to require users to change passwords at least once every 90 days. |  | | | | | |
| **8.2.4.b** ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that:   * Non-consumer customer user passwords are required to change periodically; and * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that:   * Non-consumer customer user passwords are required to change periodically; and * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change. |  | | | | | |
| **Describe how** internal processes were reviewed to verify that: | | | | | | |
| * Non-consumer customer user passwords are required to change periodically; and |  | | | | | |
| * Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change. |  | | | | | |
| **8.2.5** Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings were inspected to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. |  | | | | | |
| **8.2.5.b** ***Additional Procedure for service provider assessments only:*** Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords cannot be the same as the previous four passwords. | *Additional procedure for service provider assessments only,***identify the documented internal processes and customer/user documentation** reviewed to verify that new non-consumer customer user passwords cannot be the same as the previous four passwords. |  | | | | | |
| **Describe how** internal processes were reviewed to verify that new non-consumer customer user passwords cannot be the same as the previous four passwords. |  | | | | | |
| **8.2.6** Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use. | **Identify** **the documented password procedures** examined to verify the procedures define that:   * First-time passwords must be set to a unique value for each user. * First-time passwords must be changed after the first use. * Reset passwords must be set to a unique value for each user. * Reset passwords must be changed after the first use. |  | | | | | |
| **Describe how** security personnel were observed to: | | | | | | |
| * Set first-time passwords to a unique value for each new user. |  | | | | | |
| * Set first-time passwords to be changed after first use. |  | | | | | |
| * Set reset passwords to a unique value for each existing user. |  | | | | | |
| * Set reset passwords to be changed after first use. |  | | | | | |
| **8.3** Incorporate two-factor authentication for remote network access originating from outside the network, by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).  **Note:** Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.  Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.3.a** Examine system configurations for remote access servers and systems to verify two-factor authentication is required for:   * All remote access by personnel. * All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). | **Describe how** system configurations for remote access servers and systems were examined to verify two-factor authentication is required for: | | | | | | |
| * All remote access by personnel. |  | | | | | |
| * All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). |  | | | | | |
| **8.3.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. | **Identify the sample of personnel** observed connecting remotely to the network selected. |  | | | | | |
| *For each item in the sample,* **describe how** two-factor authentication was observed to be required for remote access to the network. |  | | | | | |
| **Identify** which two factors are used:   * Something you know * Something you are * Something you have |  | | | | | |
| **8.4** Document and communicate authentication policies and procedures to all users including:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions not to reuse previously used passwords. * Instructions to change passwords if there is any suspicion the password could be compromised. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.4.a** Examineprocedures and interview personnel to verify that authentication policies and procedures are distributed to all users. | **Identify** **the documented policies and procedures** examined to verify authentication procedures define that authentication procedures and policies are distributed to all users. |  | | | | | |
| **Identify the personnel** interviewed who confirm that authentication policies and procedures are distributed to all users. |  | | | | | |
| **8.4.b** Review authentication policies and procedures that are distributed to users and verify they include:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions for users not to reuse previously used passwords. * Instructions to change passwords if there is any suspicion the password could be compromised. | **Identify the documented authentication policies and procedures that** **are distributed to users** reviewed to verify they include:   * Guidance on selecting strong authentication credentials. * Guidance for how users should protect their authentication credentials. * Instructions for users not to reuse previously used passwords. * That users should change passwords if there is any suspicion the password could be compromised. |  | | | | | |
| **8.4.c** Interview a sample of users to verify that they are familiar with authentication policies and procedures. | **Identify** **the sample** of users interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that the sampled users are familiar with authentication policies and procedures. |  | | | | | |
| **8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:   * Generic user IDs are disabled or removed. * Shared user IDs do not exist for system administration and other critical functions. * Shared and generic user IDs are not used to administer any system components. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.5.a** For a sample of system components, examine user ID lists to verify the following:   * Generic user IDs are disabled or removed. * Shared user IDs for system administration activities and other critical functions do not exist. * Shared and generic user IDs are not used to administer any system components. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** user ID lists for the sample of system components were examined to verify that: | | | | | | |
| * Generic user IDs are disabled or removed. |  | | | | | |
| * Shared user IDs for system administration activities and other critical functions do not exist. |  | | | | | |
| * Shared and generic user IDs are not used to administer any system components. |  | | | | | |
| **8.5.b** Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. | **Identify** **the documented policies and procedures** examined to verify authentication policies/procedures define that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. |  | | | | | |
| **8.5.c** Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. | **Identify** **the system administrators** interviewed who confirm that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. |  | | | | | |
| **8.5.1** ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.  This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.  **Note:** Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.5.1** ***Additional procedure for service providerassessments only:*** Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer. | *Additional procedure for service provider assessments only*, **indicate whether** this ROC is being completed prior to June 30, 2015**. (yes/no)** |  | | | | | |
| *If “yes” AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark this as “Not Applicable.”  *If “no” OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | |
| **Identify** **the documented procedures** examined to verify that different authentication credentials are used for access to each customer. |  | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details discussed** to confirm that different authentication credentials are used for access to each customer. |  | | | | | |
| **8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows:   * Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.6.a** Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include:   * Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. | **Identify** **the documented authentication policies and procedures** examined to verify the procedures for using authentication mechanisms define that:   * Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. * Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. |  | | | | | |
| **8.6.b** Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts. | **Identify the security personnel** interviewed who confirm that authentication mechanisms are assigned to an account and not shared among multiple accounts. |  | | | | | |
| **8.6.c** Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access. | **Identify the sample** of system components selected for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** system configuration settings and/or physical controls, as applicable, were examined to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access. |  | | | | | |
| **8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:   * All user access to, user queries of, and user actions on databases are through programmatic methods. * Only database administrators have the ability to directly access or query databases. * Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.7.a** Review database and application configuration settings and verify that all users are authenticated prior to access. | **Identify** all databases containing cardholder data. |  | | | | | |
| **Describe how** authentication is managed (for example, via application and/or database interfaces). |  | | | | | |
| **Describe how** database and/or application configuration settings were observed to verify that all users are authenticated prior to access. |  | | | | | |
| **8.7.b** Examine database and application configuration settings to verify thatall user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). | *For each database from 8.7.a:* | | | | | | |
| **Describe how** the database and application configuration settings were examined to verify that only programmatic methods are used for: | | | | | | |
| * All user access to the database |  | | | | | |
| * All user queries of the database |  | | | | | |
| * All user actions on the database |  | | | | | |
| **Describe** the process observed to verify that only programmatic methods are used for: | | | | | | |
| * All user access to the database |  | | | | | |
| * All user queries of the database |  | | | | | |
| * All user actions on the database |  | | | | | |
| **8.7.c** Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators. | *For each database from 8.7.a,* **describe how** database application configuration settings were examined to verify that the following are restricted to only database administrators: | | | | | | |
| * User direct access to databases |  | | | | | |
| * Queries of databases |  | | | | | |
| **8.7.d** Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes). | *For each database from 8.7.a:* | | | | | | |
| * **Identify** applications with access to the database. |  | | | | | |
| * **Describe** the implemented methods for ensuring that application IDs can only be used by the applications. |  | | | | | |
| * **Describe how** database access control settings, database application configuration settings and related application IDs were examined together to verify that application IDs can only be used by the applications. |  | | | | | |
| **8.8** Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.8** Examine documentation and interview personnel to verify that security policies and operational procedures for identification and authentication are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for identification and authentication are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for identification and authentication are:   * In use * Known to all affected parties |  | | | | | |

### Requirement 9: Restrict physical access to cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | | | | | **Summary of Assessment Findings**  (check one) | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | | **In Place w/CCW** | | **N/A** | **Not Tested** | | | | | | | | **Not in Place** | | |
| **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | | | | | | | ☐ | | ☐ | | ☐ | ☐ | | | | | | | | ☐ | | |
| **9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.   * Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. * Observe a system administrator’s attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are “locked” to prevent unauthorized use. | **Identify and briefly describe** all of the following with systems in the cardholder data environment: | | | | | | | | | | | | | | | | | | | | | |
| * All computer rooms |  | | | | | | | | | | | | | | | | | | | | |
| * All data centers |  | | | | | | | | | | | | | | | | | | | | |
| * Any other physical areas |  | | | | | | | | | | | | | | | | | | | | |
| *For each area identified (add rows as needed),* complete the following: | | | | | | | | | | | | | | | | | | | | | |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  | | | | | | | | | | | | | | | | | | | | |
| **Identify** the randomly selected systems in the cardholder environment for which a system administrator login attempt was observed. |  | | | | | | | | | | | | | | | | | | | | |
| **Describe how** consoles for the randomly selected systems were observed to verify that they are “locked” when not in use to prevent unauthorized use. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.1** Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.  **Note:** “Sensitive areas” refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store. | | | | | | | ☐ | | ☐ | | ☐ | ☐ | | | | | ☐ | | | | | |
| **9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas. | **Describe** the video cameras and/or access control mechanisms observed to monitor the entry/exit points to sensitive areas. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.1.b** Verify that video cameras and/or access control mechanisms are protected from tampering or disabling. | **Describe how** the video cameras and/or access control mechanisms were observed to be protected from tampering and/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. | **Describe how** the data from video cameras and/or access control mechanisms were observed to be reviewed. |  | | | | | | | | | | | | | | | | | | | | |
| **Describe how** data was observed to be stored for at least three months. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.2** Implement physical and/or logical controls to restrict access to publicly accessible network jacks.  For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks. | | | | | | | ☐ | | ☐ | | ☐ | ☐ | | | | | ☐ | | | | | |
| **9.1.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly-accessible network jacks. | **Identify responsible personnel** interviewed who confirm that physical and/or logical controls are in place to restrict access to publicly accessible network jacks. |  | | | | | | | | | | | | | | | | | | | | |
| **Describe** the physical and/or logical controls observed at the locations of publicly accessible network jacks to verify the controls are in place restrict access. |  | | | | | | | | | | | | | | | | | | | | |
| **9.1.3** Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. | | | | | | | ☐ | | ☐ | | ☐ | | ☐ | | | | ☐ | | | | | |
| **9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted. | **Describe how** physical access was observed to be restricted to the following: | | | | | | | | | | | | | | | | | | | | | |
| * Wireless access points | |  | | | | | | | | | | | | | | | | | | | |
| * Wireless gateways | |  | | | | | | | | | | | | | | | | | | | |
| * Wireless handheld devices | |  | | | | | | | | | | | | | | | | | | | |
| * Network/communications hardware | |  | | | | | | | | | | | | | | | | | | | |
| * Telecommunication lines | |  | | | | | | | | | | | | | | | | | | | |
| **9.2** Develop procedures to easily distinguish between onsite personnel and visitors, to include:   * Identifying onsite personnel and visitors (for example, assigning badges). * Changes to access requirements. * Revoking or terminating onsite personnel and expired visitor identification (such as ID badges). | | | | | | | ☐ | ☐ | | ☐ | | | ☐ | | ☐ | | | | | | | |
| **9.2.a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.  Verify procedures include the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | **Identify** **the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | |  | | | | | | | | | | | | | | | | | | | |
| **9.2.b** Examine identification methods (such as ID badges) andobserve processes for identifying and distinguishing between onsite personnel and visitors to verify that:   * Visitors are clearly identified, and * It is easy to distinguish between onsite personnel and visitors. | **Identify** the identification methods examined. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that: | | | | | | | | | | | | | | | | | | | | | |
| * Visitors are clearly identified, and | |  | | | | | | | | | | | | | | | | | | | |
| * It is easy to distinguish between onsite personnel and visitors. | |  | | | | | | | | | | | | | | | | | | | |
| **9.2.c** Verify that access to the identification process (such as a badge system) is limited to authorized personnel. | **Identify** **the document** that defines that access to the identification process is limited to authorized personnel. | |  | | | | | | | | | | | | | | | | | | | |
| **Describe how** access to the identification process was observed to be limited to authorized personnel. | |  | | | | | | | | | | | | | | | | | | | |
| **9.3** Control physical access for onsite personnel to sensitive areas as follows:   * Access must be authorized and based on individual job function. * Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | ☐ | | | | | | |
| **9.3.a** For a sample of onsite personnel with physical access to sensitive areas, interview responsible personnel and observe access control lists to verify that:   * Access to the sensitive area is authorized. * Access is required for the individual’s job function. | **Identify the sample** of onsite personnel with physical access to sensitive areas interviewed for this testing procedure. | | |  | | | | | | | | | | | | | | | | | | |
| *For all items in the sample,* **describe how** responsible personnel were interviewed and access control lists observed to verify that: | | | | | | | | | | | | | | | | | | | | | |
| * Access to the sensitive area is authorized. | | |  | | | | | | | | | | | | | | | | | | |
| * Access is required for the individual’s job function. | | |  | | | | | | | | | | | | | | | | | | |
| **9.3.b** Observe personnel accessing sensitive areas to verify that all personnel are authorized before being granted access. | **Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access. | | |  | | | | | | | | | | | | | | | | | | |
| **9.3.c** Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas. | **Identify** **the sample** of users recently terminated. | | |  | | | | | | | | | | | | | | | | | | |
| *For all items in the sample,* **provide the name of the assessor** who attests that the access control lists were reviewed to verify the personnel do not have physical access to sensitive areas. | | |  | | | | | | | | | | | | | | | | | | |
| **9.4** Implement procedures to identify and authorize visitors.  Procedures should include the following: | | | | | | | | | | | | | | | | | | | | | | |
| **9.4** Verify that visitor authorization and access controls are in place as follows: | | | | | | | | | | | | | | | | | | | | | | |
| **9.4.1** Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | ☐ | | | | | | | |  |
| **9.4.1.a** Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. | **Describe how** visitor authorization processes were observed to verify that visitors:   * Must be authorized before they are granted access to areas where cardholder data is processed or maintained. * Are escorted at all times within areas where cardholder data is processed and maintained. | | |  | | | | | | | | | | | | | | | | | | |
| **Identify personnel** interviewed who confirm that visitor authorization processes are in place so that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. | | |  | | | | | | | | | | | | | | | | | | |
| **9.4.1.b** Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. | **Describe how** the use of visitor badges or other identification was observed to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. | | |  | | | | | | | | | | | | | | | | | | |
| **9.4.2** Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | ☐ | | | |  |
| **9.4.2.a** Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel. | **Describe how** people within the facility were observed to use visitor badges or other identification. | | | |  | | | | | | | | | | | | | | | | | |
| **Describe how** visitors within the facility were observed to be easily distinguishable from onsite personnel. | | | |  | | | | | | | | | | | | | | | | | |
| **9.4.2.b** Verify that visitor badges or other identification expire. | **Describe how** visitor badges or other identification were verified to expire. | | | |  | | | | | | | | | | | | | | | | | |
| **9.4.3** Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.4.3** Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration. | **Describe how** visitors leaving the facility were observed to verify they are asked to surrender their badge or other identification upon departure or expiration. | | | |  | | | | | | | | | | | | | | | | | |
| **9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.  Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log.  Retain this log for a minimum of three months, unless otherwise restricted by law. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.4.4.a** Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. | **Describe how** it was verified that a visitor log is in use to record physical access to: | | | | | | | | | | | | | | | | | | | | | |
| * The facility. | | | | |  | | | | | | | | | | | | | | | | |
| * Computer rooms and data centers where cardholder data is stored or transmitted. | | | | |  | | | | | | | | | | | | | | | | |
| **9.4.4.b** Verify that the log contains:   * The visitor’s name, * The firm represented, and * The onsite personnel authorizing physical access. | **Provide the name of the assessor** who attests that the visitor log contains:   * The visitor’s name, * The firm represented, and * The onsite personnel authorizing physical access. | | | | |  | | | | | | | | | | | | | | | | |
| **9.4.4.c** Verify that the log is retained for at least three months. | **Identify** the defined retention period for visitor logs. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** visitor logs were observed to be retained for at least three months. | | | | |  | | | | | | | | | | | | | | | | |
| **9.5** Physically secure all media. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.5** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). | **Identify the documented procedures for protecting cardholder data** reviewed to verify controls for physically securing all media are defined. | | | | |  | | | | | | | | | | | | | | | | |
| *For all types of media used,* **describe the controls** for physically securing the media used. | | | | |  | | | | | | | | | | | | | | | | |
| **9.5.1** Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location’s security at least annually. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.5.1.a** Observe the storage location’s physical security to confirm that backup media storage is secure. | **Identify** **all locations** where backup media is stored. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** it was observed that backup media storage is stored in a secure location. | | | | |  | | | | | | | | | | | | | | | | |
| **9.5.1.b** Verify that the storage location security is reviewed at least annually. | **Identify** **the document** reviewed to verify that the storage location must be reviewed at least annually. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** processes were observed to verify that reviews of the security of each storage location are performed at least annually. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6** Maintain strict control over the internal or external distribution of any kind of media, including the following: | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.6** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | **Identify** **the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** media distribution is controlled, including distribution to individuals. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6.1** Classify media so the sensitivity of the data can be determined. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.6.1** Verify that all media is classified so the sensitivity of the data can be determined. | **Identify the documented policy** reviewed to verify policy defines how media is classified. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** the classifications were observed to be implemented so the sensitivity of the data can be determined. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6.2** Send the media by secured courier or other delivery method that can be accurately tracked. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.6.2.a** Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. | **Identify** **the personnel** interviewed who confirm that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. | | | | |  | | | | | | | | | | | | | | | | |
| **Identify the record**s examined for this testing procedure. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** offsite tracking records were examined to verify that all media is logged and sent via secured courier or other delivery method that can be tracked. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6.2.b** Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented. | **Identify the sample** of recent offsite tracking logs for all media selected. | | | | |  | | | | | | | | | | | | | | | | |
| *For each item in the sample,* **describe how** the offsite tracking logs were reviewed to verify that tracking details are documented. | | | | |  | | | | | | | | | | | | | | | | |
| **9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.6.3** Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | **Identify** **responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | | | | |  | | | | | | | | | | | | | | | | |
| *For each item in the sample in 9.6.2.b,* **describe how** offsite tracking logs were examined to verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). | | | | |  | | | | | | | | | | | | | | | | |
| **9.7** Maintain strict control over the storage and accessibility of media. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.7** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories. | **Identify the documented policy** **for controlling storage and maintenance of all media** that was reviewed to verify that the policy defines required periodic media inventories. | | | | |  | | | | | | | | | | | | | | | | |
| **9.7.1** Properly maintain inventory logs of all media and conduct media inventories at least annually. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.7.1** Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually. | **Identify the media inventories logs** reviewed. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** the media inventory logs were reviewed to verify that: | | | | | | | | | | | | | | | | | | | | | |
| * Media inventory logs of all media were observed to be maintained. | | | | |  | | | | | | | | | | | | | | | | |
| * Media inventories are performed at least annually. | | | | |  | | | | | | | | | | | | | | | | |
| **9.8** Destroy media when it is no longer needed for business or legal reasons as follows: | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | ☐ | | |  |
| **9.8** Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | **Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | | | | |  | | | | | | | | | | | | | | | | |
| **9.8.1** Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.8.1.a** Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | **Identify** **personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** the procedures were examined to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. | | | | |  | | | | | | | | | | | | | | | | |
| **9.8.1.b** Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured. | **Describe how** the storage containers used for materials to be destroyed are secured. | | | | |  | | | | | | | | | | | | | | | | |
| **9.8.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.8.2** Verify that cardholder data on electronic media is rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). | **Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media. | | | | |  | | | | | | | | | | | | | | | | |
| If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify the industry-accepted standards** used. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9** Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.  **Note:** These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.  **Note:** Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.9** Examine documented policies and procedures to verify they include:   * Maintaining a list of devices. * Periodically inspecting devices to look for tampering or substitution. * Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. | **Indicate whether** this ROC is being completed prior to June 30, 2015**. (yes/no)** | | | | |  | | | | | | | | | | | | | | | | |
| *If “yes” AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark 9.9 – 9.9.3.b as “Not Applicable.”  *If not OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | | | | | | | | | | | | | | | | |
| **Identify the documented policies and procedures** examined to verify they include:   * Maintaining a list of devices. * Periodically inspecting devices to look for tampering or substitution. * Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.1** Maintain an up-to-date list of devices. The list should include the following:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.9.1.a** Examine the list of devices to verify it includes:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | *If “yes” at 9.9 AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark 9.9.1.a -9.9.1.c as “Not Applicable.”  *If not OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | | | | | | | | | | | | | | | | |
| **Identify the documented up-to-date list of devices** examined to verify it includes:   * Make, model of device. * Location of device (for example, the address of the site or facility where the device is located). * Device serial number or other method of unique identification. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.1.b** Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up-to-date. | **Identify the sample** of devices from the list selected for this testing procedure. | | | | |  | | | | | | | | | | | | | | | | |
| *For all items in the sample,* **describe how** the devices and device locations for the sample of devices were observed to verify that the list is accurate and up-to-date. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.1.c** Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc. | **Identify personnel** interviewed for this testing procedure. | | | | |  | | | | | | | | | | | | | | | | |
| For the interview, **summarize the relevant details** discussed that verify the list of devices is updated when devices are added, relocated, decommissioned, etc. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.2** Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).  **Note:** Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.9.2.a** Examine documented procedures to verify processes are defined to include the following:   * Procedures for inspecting devices. * Frequency of inspections. | *If “yes” at 9.9 AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark 9.9.2.a -9.9.2.b as “Not Applicable.”  *If not OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | | | | | | | | | | | | | | | | |
| **Identify** **the documented procedures** examined to verify that processes are defined to include the following:   * Procedures for inspecting devices. * Frequency of inspections. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.2.b** Interview responsible personnel and observe inspection processes to verify:   * Personnel are aware of procedures for inspecting devices. * All devices are periodically inspected for evidence of tampering and substitution. | **Identify** **responsible personnel** interviewed who confirm that:   * Personnel are aware of procedures for inspecting devices. * All devices are periodically inspected for evidence of tampering and substitution. | | | | |  | | | | | | | | | | | | | | | | |
| **Describe how** inspection processes were observed to verify that: | | | | | | | | | | | | | | | | | | | | | |
| * All devices are periodically inspected for evidence of tampering. | | | | |  | | | | | | | | | | | | | | | | |
| * All devices are periodically inspected for evidence of substitution. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.3** Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:   * Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Do not install, replace, or return devices without verification. * Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.9.3.a** Review training materials for personnel at point-of-sale locations to verify it includes training in the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | *If “yes” at 9.9 AND the assessed entity does not have this in place ahead of the requirement’s effective date,* mark 9.9.3.a -9.9.3.b as “Not Applicable.”  *If not OR if the assessed entity has this in place ahead of the requirement’s effective date,* complete the following*:* | | | | | | | | | | | | | | | | | | | | | |
| **Identify** **the training materials for personnel at point-of-sale locations** that were reviewed to verify the materials include training in the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting all suspicious behavior to appropriate personnel (for example, a manager or security officer). * Reporting tampering or substitution of devices. | | | | |  | | | | | | | | | | | | | | | | |
| **9.9.3.b** Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following:   * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. * Not to install, replace, or return devices without verification. * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | **Identify** **the sample** of personnel at point-of-sale locations interviewed to verify they have received training. | | | | |  | | | | | | | | | | | | | | | | |
| For the interview, **summarize the relevant details** discussed that verify interviewees are aware of the procedures for the following: | | | | | | | | | | | | | | | | | | | | | |
| * Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. | | | | |  | | | | | | | | | | | | | | | | |
| * Not to install, replace, or return devices without verification. | | | | |  | | | | | | | | | | | | | | | | |
| * Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). | | | | |  | | | | | | | | | | | | | | | | |
| * Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | | | | |  | | | | | | | | | | | | | | | | |
| **9.10** Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. | | | | | | | ☐ | ☐ | | | ☐ | | ☐ | | | | | | | | ☐ | |
| **9.10** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document reviewed to** verify that security policies and operational procedures for restricting physical access to cardholder data are documented. | | | | |  | | | | | | | | | | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for restricting physical access to cardholder data are: | | | | | | | | | | | | | | | | | | | | | |
| * In use | | | | |  | | | | | | | | | | | | | | | | |
| * Known to all affected parties | | | | |  | | | | | | | | | | | | | | | | |

## Regularly Monitor and Test Networks

### Requirement 10: Track and monitor all access to network resources and cardholder data

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | | | **In Place w/ CCW** | **N/A** | | **Not Tested** | | | | **Not in Place** |
| **10.1** Implement audit trails to link all access to system components to each individual user. | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.1** Verify, through observation and interviewing the system administrator, that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. | **Identify the system administrator(s)** interviewed who confirm that:   * Audit trails are enabled and active for system components. * Access to system components is linked to individual users. |  | | | | | | | | | | | |
| **Describe how** audit trails were observed to verify the following: | | | | | | | | | | | | |
| * Audit trails are enabled and active for system components. |  | | | | | | | | | | | |
| * Access to system components is linked to individual users. |  | | | | | | | | | | | |
| **10.2** Implement automated audit trails for all system components to reconstruct the following events: | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following: | **Identify the responsible personnel** interviewed who confirm the following from 10.2.1-10.2.7 are logged:   * All individual access to cardholder data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  | | | | | | | | | | | |
|  | **Identify the sample of audit logs** observed to verify the following from 10.2.1-10.2.7 are logged:   * All individual access to cardholder data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including.   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  | | | | | | | | | | | |
| **10.2.1** All individual user accesses to cardholder data. | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.2.1** Verify all individual access to cardholder data is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify all individual access to cardholder data is logged. |  | | | | | | | | | | | |
| **10.2.2** All actions taken by any individual with root or administrative privileges. | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.2.2** Verify all actions taken by any individual with root or administrative privileges are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify all actions taken by any individual with root or administrative privileges are logged. |  | | | | | | | | | | | |
| **10.2.3** Access to all audit trails. | | | ☐ | | | ☐ | ☐ | | ☐ | | | | ☐ |
| **10.2.3** Verify access to all audit trails is logged. | *For all items in the sample at 10.2*, **describe how** configuration settings were observed to verify access to all audit trails is logged. |  | | | | | | | | | | | |
| **10.2.4** Invalid logical access attempts. | | | | ☐ | ☐ | | ☐ | | ☐ | | | | ☐ |
| **10.2.4** Verify invalid logical access attempts are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify invalid logical access attempts are logged. |  | | | | | | | | | | | |
| **10.2.5** Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.2.5.a** Verify use of identification and authentication mechanisms is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify use of identification and authentication mechanisms is logged. |  | | | | | | | | | | | |
| **10.2.5.b** Verify all elevation of privileges is logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify all elevation of privileges is logged. |  | | | | | | | | | | | |
| **10.2.5.c** Verify all changes, additions, or deletions to any account with root or administrative privileges are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify all changes, additions, or deletions to any account with root or administrative privileges are logged. |  | | | | | | | | | | | |
| **10.2.6** Initialization, stopping, or pausing of the audit logs. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.2.6** Verify the following are logged:   * Initialization of audit logs. * Stopping or pausing of audit logs. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify initialization of audit logs is logged. |  | | | | | | | | | | | |
| *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify stopping and pausing of audit logs is logged. |  | | | | | | | | | | | |
| **10.2.7** Creation and deletion of system-level objects. | | | | ☐ | ☐ | | | ☐ | | ☐ | ☐ | | |
| **10.2.7** Verify creation and deletion of system level objects are logged. | *For all items in the sample at 10.2,* **describe how** configuration settings were observed to verify creation and deletion of system level objects are logged. |  | | | | | | | | | | | |
| **10.3** Record at least the following audit trail entries for all system components for each event: | | | | ☐ | ☐ | | | ☐ | | ☐ | ☐ | | |
| **10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following: | **Identify the responsible personnel** interviewed who confirm that for each auditable event from 10.2.1-10.2.7, the following are included in log entries:   * User identification * Type of event * Date and time * Success or failure indication * Origination of event |  | | | | | | | | | | | |
| **Identify the sample of audit logs** from 10.2.1-10.2.7 observed to verify the following are included in log entries:   * User identification * Type of event * Date and time * Success or failure indication * Origination of event |  | | | | | | | | | | | |
| **10.3.1** User identification | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.1** Verify user identification is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify user identification is included in log entries. |  | | | | | | | | | | | |
| **10.3.2** Type of event | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.2** Verify type of event is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify type of event is included in log entries. |  | | | | | | | | | | | |
| **10.3.3** Date and time | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.3** Verify date and time stamp is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify date and time stamp is included in log entries. |  | | | | | | | | | | | |
| **10.3.4** Success or failure indication | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.4** Verify success or failure indication is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify success or failure indication is included in log entries. |  | | | | | | | | | | | |
| **10.3.5** Origination of event | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.5** Verify origination of event is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify origination of event is included in log entries. |  | | | | | | | | | | | |
| **10.3.6** Identity or name of affected data, system component, or resource | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries. | *For all logs in the sample at 10.3,* **describe how** the audit logs were observed to verify the identity or name of affected data, system component, or resource is included in log entries. |  | | | | | | | | | | | |
| **10.4** Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.  ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).* | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. | **Identify** the time synchronization technologies in use. (If NTP, include version) |  | | | | | | | | | | | |
| **Identify** **the documented time-synchronization process** that defines processes for ensuring the time synchronization technologies are kept current per PCI DSS Requirements 6.1 and 6.2. |  | | | | | | | | | | | |
| **Describe how** processes were examined to verify that time synchronization technologies are: | | | | | | | | | | | | |
| * Implemented. |  | | | | | | | | | | | |
| * Kept current, per the documented process. |  | | | | | | | | | | | |
| **10.4.1** Critical systems have the correct and consistent time. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. * Systems receive time information only from designated central time server(s). | **Identify** **the documented process for acquiring, distributing, and storing the correct time within the organization** examined to verify that the process defines the following:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the time servers peer with one another to keep accurate time. * Systems receive time information only from designated central time server(s). |  | | | | | | | | | | | |
| **10.4.1.b** Observe the time-related system-parameter settings for a sample of system components to verify:   * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. * Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. * Systems receive time only from designated central time server(s). | **Identify the sample** of system components selected for 10.4.1.b-10.4.2.b |  | | | | | | | | | | | |
| *For all items in the sample,* **describe how** the time-related system-parameter settings for the sample of system components were observed to verify: | | | | | | | | | | | | |
| * Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. |  | | | | | | | | | | | |
| * Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. |  | | | | | | | | | | | |
| * Systems receive time only from designated central time server(s). |  | | | | | | | | | | | |
| **10.4.2** Time data is protected. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data. | **Identify the documented time-synchronization procedures** examined to verify procedures define that:   * Access to time data is restricted to only personnel with a business need to access time data. * Define which personnel have a business need to access time data. |  | | | | | | | | | | | |
| **Identify** **the authorized personnel** interviewed who confirm that personnel with access to time data have a business need to access time data. |  | | | | | | | | | | | |
| *For all items in the sample from 10.4.1,* **describe how** configuration settings were examined to restrict access to time data to only personnel with a documented need. |  | | | | | | | | | | | |
| **10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. | **Identify the documented time-synchronization procedures** examined to verify procedures define that changes to time settings on critical systems must be:   * Logged * Monitored * Reviewed |  | | | | | | | | | | | |
| *For all items in the sample from 10.4.1,* **describe how** configuration settings on the sampled system components were examined to log any changes to time settings on critical systems. |  | | | | | | | | | | | |
| *For all items in the sample from 10.4.1,* **describe how** logs were examined to log any changes to time settings on critical systems. |  | | | | | | | | | | | |
| **Describe how** time synchronization processes were examined to verify changes to time settings on critical systems are: | | | | | | | | | | | | |
| * Logged |  | | | | | | | | | | | |
| * Monitored |  | | | | | | | | | | | |
| * Reviewed |  | | | | | | | | | | | |
| **10.4.3** Time settings are received from industry-accepted time sources. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers). | **Identify** **the document** reviewed to verify it defines that:   * Time settings are configured to either accept time updates from specific, industry-accepted time sources; OR * The updates are encrypted with a symmetric key and access control lists specify the IP addresses of client machines that will be provided with the time updates. |  | | | | | | | | | | | |
| **Identify the sample** of time servers selected. |  | | | | | | | | | | | |
| *For all items in the sample,* **describe how** configuration settings were examined to verify either of the following: | | | | | | | | | | | | |
| * **T**hat the time servers receive time updates from specific, industry-accepted external sources. OR |  | | | | | | | | | | | |
| * That time updates are encrypted with a symmetric key, and access control lists specify the IP addresses of client machines. |  | | | | | | | | | | | |
| **Identify** the industry-accepted time source indicated (if applicable). |  | | | | | | | | | | | |
| **10.5** Secure audit trails so they cannot be altered. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5** Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows: | **Identify the system administrators** interviewed who confirm that audit trails are secured so that they cannot be altered as follows (from 10.5.1-10.5.5):   * Only individuals who have a job-related need can view audit trail files. * Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. * Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter, including: * That current audit trail files are promptly backed up to the centralized log server or media * The frequency that audit trail files are backed up * That the centralized log server or media is difficult to alter * Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. * Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. |  | | | | | | | | | | | |
| **Identify the sample** of system components selected for this testing procedure from 10.5.1-10.5.5. |  | | | | | | | | | | | |
| **10.5.1** Limit viewing of audit trails to those with a job-related need. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.1** Only individuals who have a job-related need can view audit trail files. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions were examined to verify they restrict viewing of audit trail files to only individuals who have a documented job-related need. |  | | | | | | | | | | | |
| **10.5.2** Protect audit trail files from unauthorized modifications. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.2** Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions were examined to verify that current audit trail files are protected from unauthorized modifications. (e.g., via access control mechanisms, physical segregation, and/or network segregation). |  | | | | | | | | | | | |
| **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.3** Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions were examined to verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. |  | | | | | | | | | | | |
| **Identify and briefly describe** the following: | | | | | | | | | | | | |
| * The centralized log server or media to which audit trail files are backed up. |  | | | | | | | | | | | |
| * How frequently the audit trail files are backed up, and how the frequency is appropriate. |  | | | | | | | | | | | |
| * How the centralized log server or media is difficult to alter. |  | | | | | | | | | | | |
| **10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.4** Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. | *For each item in the sample at 10.5,* **describe how** system configurations and permissions were examined to verify that logs for external-facing technologies are written onto a secure, centralized, internal log server or media. |  | | | | | | | | | | | |
| **Describe how** logs for external-facing technologies are written onto a secure centralized internal log server or media. |  | | | | | | | | | | | |
| **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.5.5** Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs. | *For each item in the sample at 10.5,* **describe how** the following were examined to verify the use of file-integrity monitoring or change-detection software on logs: | | | | | | | | | | | | |
| * System settings |  | | | | | | | | | | | |
| * Monitored files |  | | | | | | | | | | | |
| * Results from monitoring activities |  | | | | | | | | | | | |
| **Identify** the file-integrity monitoring (FIM) or change-detection software verified to be in use. |  | | | | | | | | | | | |
| **10.6** Review logs and security events for all system components to identify anomalies or suspicious activity.  **Note:** Log harvesting, parsing, and alerting tools may be used to meet this Requirement. | | | | | | | | | | | | | |
| **10.6** Perform the following: | | | | | | | | | | | | | |
| **10.6.1** Review the following at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.6.1.a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | **Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  | | | | | | | | | | | |
| **Describe** the manual or log tools used for daily review of logs. |  | | | | | | | | | | | |
| **10.6.1.b** Observe processes and interview personnel to verify that the following are reviewed at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) | **Identify the personnel** interviewed who confirm that the following are reviewed at least daily:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  | | | | | | | | | | | |
| **Describe how** processes were observed to verify that the following are reviewed at least daily: | | | | | | | | | | | | |
| * All security events. |  | | | | | | | | | | | |
| * Logs of all system components that store, process, or transmit CHD and/or SAD. |  | | | | | | | | | | | |
| * Logs of all critical system components. |  | | | | | | | | | | | |
| * Logs of all servers and system components that perform security functions. |  | | | | | | | | | | | |
| **10.6.2** Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.6.2.a** Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. | **Identify** **the documented security policies and procedures** examined to verify that procedures define reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. |  | | | | | | | | | | | |
| **Describe the manual or log tools** defined for periodic review of logs of all other system components. |  | | | | | | | | | | | |
| **10.6.2.b** Examine the organization’s risk assessment documentation and interview personnel to verify that reviews are performed in accordance with organization’s policies and risk management strategy. | **Identify** **the organization’s risk assessment documentation** examined to verify that reviews are performed in accordance with the organization’s policies and risk management strategy. |  | | | | | | | | | | | |
| **Identify** **the personnel** interviewed for this testing procedure. |  | | | | | | | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that reviews are performed in accordance with the organization’s policies and risk management strategy. |  | | | | | | | | | | | |
| **10.6.3** Follow up exceptions and anomalies identified during the review process. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. | **Identify** **the documented security policies and procedures** examined to verify that procedures define following up on exceptions and anomalies identified during the review process. |  | | | | | | | | | | | |
| **10.6.3.b** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed. | **Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed. |  | | | | | | | | | | | |
| **Identify** **the personnel** interviewed who confirm that follow-up to exceptions and anomalies is performed. |  | | | | | | | | | | | |
| **10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.7.a** Examine security policies and procedures to verify that they define the following:   * Audit log retention policies. * Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. | **Identify** **the documented security policies and procedures** examined to verify that procedures define the following:   * Audit log retention policies. * Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. |  | | | | | | | | | | | |
| **10.7.b** Interview personnel and examine audit logs to verify that audit logs are retained for at least one year. | **Identify** **the personnel** interviewed who confirm that audit logs are retained for at least one year. |  | | | | | | | | | | | |
| **Describe how** the audit logs were examined to verify that audit logs are retained for at least one year. |  | | | | | | | | | | | |
| **10.7.c** Interview personnel and observe processes to verify that at least the last three months’ logs are immediately available for analysis. | **Identify** **the personnel** interviewed who confirm that at least the last three months’ logs are immediately available for analysis. |  | | | | | | | | | | | |
| **Describe** the processes observed to verify that at least the last three months’ logs are immediately available for analysis. |  | | | | | | | | | | | |
| **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. | | | | ☐ | ☐ | | | ☐ | | ☐ | | ☐ | |
| **10.8** Examine documentation and interview personnel to verify 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. | **Identify the document** reviewed to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented. |  | | | | | | | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for monitoring all access to network resources and cardholder data are:   * In use * Known to all affected parties |  | | | | | | | | | | | |

### Requirement 11: Regularly test security systems and processes

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.  **Note:** Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.  Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.a** Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis. | **Identify** **the documented policies and procedures** examined to verify processes are defined for detection and identification of authorized and unauthorized wireless access points on a quarterly basis. |  | | | | | |
| **11.1.b** Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:   * WLAN cards inserted into system components. * Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). * Wireless devices attached to a network port or network device. | **Describe how** the methodology/processes were verified to be adequate to detect and identify unauthorized wireless access points, including the following: | | | | | | |
| * WLAN cards inserted into system components. |  | | | | | |
| * Portable or mobile devices attached to system components to create a wireless access point. |  | | | | | |
| * Wireless devices attached to a network port or network device. |  | | | | | |
| * Any other unauthorized wireless access point. |  | | | | | |
| **11.1.c If wireless scanning is utilized, e**xamine output from recent wireless scans to verify that:   * Authorized and unauthorized wireless access points are identified, and * The scan is performed at least quarterly for all system components and facilities. | **Indicate whether** wireless scanning is utilized. **(yes/no)**  *If ‘no,’ mark the remainder of 11.1.c as ‘not applicable.’* |  | | | | | |
| *If ‘yes,’* **Identify/describe** the output from recent wireless scans examined to verify that:   * Authorized wireless access points are identified. * Unauthorized wireless access points are identified. * The scan is performed at least quarterly. * The scan covers all system components. * The scan covers all facilities. |  | | | | | |
| **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel. | **Indicate** **whether** automated monitoring is utilized. **(yes/no)** |  | | | | | |
| *If “no,” mark the remainder of 11.1.d as “Not Applicable.”*  *If “yes,” complete the following:* | | | | | | |
| **Identify and describe** any automated monitoring technologies in use. |  | | | | | |
| *For each monitoring technology in use,* **describe how** the technology generates alerts to personnel. |  | | | | | |
| **11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.1** Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. | **Identify** **the documented inventory records** of authorized wireless access points examined to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. |  | | | | | |
| **11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.2.a** Examine the organization’s incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected. | **Identify the Incident Response Plan document** examined that defines and requires response in the event that an unauthorized wireless access point is detected. |  | | | | | |
| **11.1.2.b** Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found. | **Identify** **the responsible personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize the relevant details** discussed that verify that action is taken when unauthorized wireless access points are found. |  | | | | | |
| *And/or:* | | | | | | |
| **Identify the recent wireless scans** inspected for this testing procedure. |  | | | | | |
| **Describe how** the recent wireless scans and related responses were inspected to verify that action is taken when unauthorized wireless access points are found. |  | | | | | |
| **11.2** Run internal and external network vulnerability scans at least quarterly andafter any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).  **Note:** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.*  *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2** Examine scan reports and supporting documentation toverify that internal and external vulnerability scans are performed as follows: | | | | | | | |
| **11.2.1** Perform quarterly internal vulnerability scans, and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. | **Identify** **the internal vulnerability scan reports and supporting documentation** reviewed. |  | | | | | |
| **Provide the name of the assessor** who attests that four quarterly internal scans were verified to have occurred in the most recent 12-month period. |  | | | | | |
| **11.2.1.b** Review the scan reports and verify that the scan process includes rescans until all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. | **Identify the documented process for quarterly internal scanning** to verify the process defines performing rescans as part of the quarterly internal scan process. |  | | | | | |
| *For each of the four internal quarterly scans indicated at 11.2.1.a*, **indicate whether** a rescan was required. **(yes/no)** |  | | | | | |
| *If “yes,”* ***describe how*** *rescans were verified to be performed until either:* | | | | | | |
| * Passing results are obtained, or |  | | | | | |
| * All “High” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. |  | | | | | |
| **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). | **Identify the responsible personnel** interviewed who confirm that the scan was performed by a qualified internal resource(s) or qualified external third party. |  | | | | | |
| **Indicate** **whether** a qualified internal resource performs the scan. **(yes/no)**  *If “no,” mark the remainder of 11.2.1.c as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the scans demonstrated they are qualified to perform the scans. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.2.2** Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.  **Note:** Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).  Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period. | **Identify** **the external network vulnerability scan reports and supporting documentation** reviewed. |  | | | | | |
| **Provide the name of the assessor** who attests that four quarterly external vulnerability scans were verified to have occurred in the most recent 12-month period. |  | | | | | |
| **11.2.2.b** Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, no automatic failures). | **Describe how** the results of each quarterly scan were reviewed to verify that the ASV Program Guide requirements for a passing scan have been met. |  | | | | | |
| *For each of the four external quarterly scans indicated at 11.2.2.a*, **indicate whether** a rescan was necessary. **(yes/no)** |  | | | | | |
| *If “yes,”* **describe how** the results of the rescan were reviewed to verify that the ASV Program Guide requirements for a passing scan have been met. |  | | | | | |
| **11.2.2.c** Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV). | **Provide the name of the assessor** who attests that the external scan reports were reviewed and verified to have been completed by a PCI SSC-Approved Scanning Vendor (ASV). |  | | | | | |
| **11.2.3** Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.2.3.a** Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned. | **Identify the document** reviewed to verify processes are defined for performing internal and external scans after any significant change. |  | | | | | |
| **Identify the change control documentation and scan reports** reviewed for this testing procedure. |  | | | | | |
| **Describe how** the change control documentation and scan reports were inspected and correlated to verify that all system components subject to significant change were scanned after the change. |  | | | | | |
| **11.2.3.b** Review scan reports and verify that the scan process includes rescans until:   * For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. * For internal scans, all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. | For all scans reviewed in 11.2.3.a, **indicate whether** a rescan was required. **(yes/no)** |  | | | | | |
| *If “yes”* – for external scans, **describe how** rescans were performed until no vulnerabilities with a CVSS score greater than 4.0 exist. |  | | | | | |
| *If “yes”* – for internal scans, **describe how** rescans were performed until either passing results were obtained or all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 were resolved. |  | | | | | |
| **11.2.3.c** Validate 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). | **Describe how** it was validated that the scan was performed by a qualified internal resource(s) or qualified external third party. |  | | | | | |
| **Indicate whether** an **i**nternal resource performed the scans. **(yes/no)**  *If “no,” mark the remainder of 11.2.3.c as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the scans demonstrated they are qualified to perform the scans. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3 Penetration Testing**  ***Note:*** *The update to**Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.1 is in place. Do not answer both v2.0 and 3.1 reporting instructions.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Indicate whether** 11.3 for this ROC is being assessed against PCI DSS v2.0 or v3.1 (either is acceptable until June 30, 2015.) **(2.0/3.1)** | | 3.1 | | | | | |
| ***If assessing against PCI DSS v2.0 for 11.3, please complete the following section in purple:*** | | | | | | | |
| **11.3** Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: | | | ☐ | ☐ | **☑** | ☐ | ☐ |
| **11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. | * **Identify the documented penetration test results** which confirm:  1. Internal penetration tests are performed annually. 2. External penetration tests are performed annually.  * **Identify whether** any significant infrastructure or application upgrade or modification occurred during the past 12 months. * **Identify the documented penetration test results** confirming that penetration tests are performed after:  1. Significant internal infrastructure or application upgrade. 2. Significant external infrastructure or application upgrade. | Not Applicable | | | | | |
| **11.3.b** Verify that noted exploitable vulnerabilities were corrected and testing repeated. | * **Identify whether** any exploitable vulnerabilities were noted in the most recent:  1. Internal penetration test results. 2. External penetration test results.  * **Identify the interviewed personnel** who confirm that all noted exploitable vulnerabilities were corrected. * **Identify the documented penetration test results** confirming that:  1. Testing was repeated. 2. All noted exploitable vulnerabilities were corrected. | Not Applicable | | | | | |
| **11.3.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). | * **Identify whether** internal and/or external resources perform the penetration tests. * **Identify the interviewed personnel who perform the tests**, and describe how the personnel demonstrated they are qualified to perform the tests. * **Describe how** organizational independence of the tester was observed to exist. | Not Applicable | | | | | |
| **11.3.1** Network-layer penetration tests. | | | ☐ | ☐ | **☑** | ☐ | ☐ |
| **11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems. | * **Identify the documented results from the most recent penetration tests** confirming that:  1. Internal penetration testing includes network-layer penetration tests. 2. External penetration testing includes network-layer penetration tests. 3. The network-layer penetration tests include:    * Components that support network functions    * Operating systems  * **Identify the responsible personnel** interviewed who confirm that:  1. Internal penetration testing includes network-layer penetration tests. 2. External penetration testing includes network-layer penetration tests. 3. The network-layer penetration tests include:    * Components that support network functions    * Operating systems | Not Applicable | | | | | |
| **11.3.2** Application-layer penetration tests. | | | ☐ | ☐ | **☑** | ☐ | ☐ |
| **11.3.2** Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5. | * **Identify the documented results from the most recent penetration tests** confirming that:  1. Internal penetration testing includes application-layer penetration tests. 2. External penetration testing includes application-layer penetration tests. 3. The application-layer tests include, at a minimum, the vulnerabilities listed in PCI DSS Requirement 6.5.  * **Identify the responsible personnel** interviewed who confirm that:  1. Internal penetration testing includes application-layer penetration tests. 2. External penetration testing includes application-layer penetration tests. 3. The application-layer tests include, at a minimum, the vulnerabilities listed in PCI DSS Requirement 6.5. | Not Applicable | | | | | |
| **END OF PCI DSS 2.0, 11.3.** | | | | | | | |
| ***If assessing against PCI DSS v3.1 for 11.3, please complete the following:*** | | | | | | | |
| **11.3** Implement a methodology for penetration testing that includes at least the following:   * Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). * Includes coverage for the entire CDE perimeter and critical systems. * Includes testing from both inside and outside of the network. * Includes testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. * Specifies retention of penetration testing results and remediation activities results.   **Note:** This update toRequirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. Prior to this date, PCI DSS v2.0 requirements for penetration testing must be followed until version 3 is in place. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3** Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented and includes at least the following:   * Is based on industry-accepted penetration testing approaches. * Includes coverage for the entire CDE perimeter and critical systems. * Includes testing from both inside and outside the network. * Includes testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. * Specifies retention of penetration testing results and remediation activities results. | **Identify the documented penetration-testing methodology** examined to verify a methodology is implemented that includes at least the following:   * Based on industry-accepted penetration testing approaches. * Coverage for the entire CDE perimeter and critical systems. * Testing from both inside and outside the network. * Testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Review and consideration of threats and vulnerabilities experienced in the last 12 months. * Retention of penetration testing results and remediation activities results. |  | | | | | |
|  | **Identify the responsible personnel** interviewed who confirm the penetration–testing methodology implemented includes at least the following:   * Based on industry-accepted penetration testing approaches. * Coverage for the entire CDE perimeter and critical systems. * Testing from both inside and outside the network. * Testing to validate any segmentation and scope reduction controls. * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. * Defines network-layer penetration tests to include components that support network functions as well as operating systems. * Review and consideration of threats and vulnerabilities experienced in the last 12 months. * Retention of penetration testing results and remediation activities results. |  | | | | | |
|  | **Describe how** the penetration-testing methodology was examined to verify that the implemented methodology includes at least the following: | | | | | | |
| * Based on industry-accepted penetration testing approaches. |  | | | | | |
| * Coverage for the entire CDE perimeter and critical systems. |  | | | | | |
| * Testing from both inside the network, and from outside of the network attempting to get in. |  | | | | | |
| * Testing to validate any segmentation and scope-reduction controls. |  | | | | | |
| * Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. |  | | | | | |
| * Defines network-layer penetration tests to include components that support network functions as well as operating systems. |  | | | | | |
| * Review and consideration of threats and vulnerabilities experienced in the last 12 months. |  | | | | | |
| * Retention of penetration testing results and remediation activities results. |  | | | | | |
| **11.3.1** Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.1.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows:   * Per the defined methodology * At least annually * After any significant changes to the environment | **Identify the documented external penetration test results** reviewed to verify that external penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Describe how** the scope of work was reviewed to verify that external penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Identify whether** any significant external infrastructure or application upgrade or modification occurred during the past 12 months. |  | | | | | |
| **Identify** **the documented penetration test results reviewed** to verify that external penetration tests are performed after significant external infrastructure or application upgrade. |  | | | | | |
| **11.3.1.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). | **Describe how** it was validated that the test was performed by a qualified internal resource(s) or qualified external third party. |  | | | | | |
| **Indicate whether** an **i**nternal resource performed the test. **(yes/no)**  *If “no,” mark the remainder of 11.3.1.b as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests. |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.2** Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows:   * Per the defined methodology * At least annually * After any significant changes to the environment | **Identify the documented internal penetration test results** reviewed to verify that internal penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Describe how** the scope of work was reviewed to verify that internal penetration testing is performed:   * Per the defined methodology * At least annually |  | | | | | |
| **Indicate whether** any significant internal infrastructure or application upgrade or modification occurred during the past 12 months. **(yes/no)** |  | | | | | |
| **Identify** **the documented internal penetration test results** reviewed to verify that internal penetration tests are performed after significant internal infrastructure or application upgrade. |  | | | | | |
| **11.3.2.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). | **Describe how** it was validated that the test was performed by a qualified internal resource(s) or qualified external third party. |  | | | | | |
| **Indicate whether** an **i**nternal resource performed the test. **(yes/no)**  *If “no,” mark the remainder of 11.3.2.b as “Not Applicable.”*  *If “yes,” complete the following:* |  | | | | | |
| **Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests |  | | | | | |
| **Describe how** organizational independence of the tester was observed to exist. |  | | | | | |
| **11.3.3** Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.3.3** Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. | **Identify the documented penetration testing results** examined to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. |  | | | | | |
| **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. | **Indicate** **whether** segmentation is used to isolate the CDE from other networks. **(yes/no)**  *If “no,” mark the remainder of 11.3.4.a and 11.3.4.b as “Not Applicable.”* |  | | | | | |
| *If “yes,”* **Describe** segmentation controls examined for this testing procedure. |  | | | | | |
| **Describe how** the segmentation controls and penetration-testing methodology were examined to verify that penetration testing procedures are defined to: | | | | | | |
| * Test all segmentation methods to confirm they are operational and effective. |  | | | | | |
| * Isolate all out-of-scope systems from systems in the CDE. |  | | | | | |
| **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. | **Identify the documented results from the most recent penetration test** examined 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. |  | | | | | |
| **11.4** Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.  Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. | **Identify the network diagrams** examined to verify that techniques are in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. |  | | | | | |
| **Identify** the techniques observed to be in place to monitor all traffic:   * At the perimeter of the cardholder data environment. * At critical points in the cardholder data environment. |  | | | | | |
| **Describe how** system configurations were examined to verify that techniques are in place to monitor all traffic: | | | | | | |
| * At the perimeter of the cardholder data environment. |  | | | | | |
| * At critical points in the cardholder data environment. |  | | | | | |
| **11.4.b** Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises. | **Describe how** system configurations for intrusion-detection, and/or intrusion-prevention techniques were examined to verify they are configured to alert personnel of suspected compromises. |  | | | | | |
| **Describe how** alerts to personnel are generated. |  | | | | | |
| **Identify the responsible personnel** interviewed who confirm that the generated alerts are received as intended. |  | | | | | |
| **11.4.c** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. | **Identify** **the vendor document(s)** examined to verify defined vendor instructions for intrusion-detection and/or intrusion-prevention techniques |  | | | | | |
| **Describe how** IDS/IPS configurations were examined and compared to vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are: | | | | | | |
| * Configured per vendor instructions to ensure optimal protection. |  | | | | | |
| * Maintained per vendor instructions to ensure optimal protection. |  | | | | | |
| * Updated per vendor instructions to ensure optimal protection. |  | | | | | |
| **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 within the cardholder data environment 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 (i.e., through risk assessment or other means)* | **Describe** the change-detection mechanism deployed. |  | | | | | |
| **Identify the results** from monitored files reviewed. |  | | | | | |
| **Describe how** change-detection mechanism settings and results from monitored files were observed to monitor changes to: | | | | | | |
| * Critical system files |  | | | | | |
| * Critical configuration files |  | | | | | |
| * Critical content files |  | | | | | |
| **11.5.b** Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly. | **Describe how** it was verified that the change-detection mechanism is configured to: | | | | | | |
| * Alert personnel to unauthorized modification (including changes, additions and deletions) of critical files. |  | | | | | |
| * Perform critical file comparisons at least weekly. |  | | | | | |
| **11.5.1** Implement a process to respond to any alerts generated by the change-detection solution. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.5.1** Interview personnel to verify that all alerts are investigated and resolved. | **Identify the personnel** interviewed for this testing procedure. |  | | | | | |
| For the interview, **summarize details of the interview** that verify that all alerts are investigated and resolved. |  | | | | | |
| **11.6** Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.6** Examine documentation and interview personnel to verify that security policies and operational procedures for security monitoring and testing are:   * Documented, * In use, and * Known to all affected parties. | **Identify the document** reviewed to verify that security policies and operational procedures for security monitoring and testing are documented. |  | | | | | |
| **Identify responsible personnel** interviewed who confirm that the above documented security policies and operational procedures for security monitoring and testing are:   * In use * Known to all affected parties |  | | | | | |

## Maintain an Information Security Policy

### Requirement 12: Maintain a policy that addresses information security for all personnel

| **PCI DSS Requirements  and Testing Procedures** | **Reporting Instruction** | **Reporting Details: Assessor’s Response** | **Summary of Assessment Findings**  (check one) | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **In Place** | **In Place w/ CCW** | **N/A** | **Not Tested** | **Not in Place** |
| **12.1** Establish, publish, maintain, and disseminate a security policy. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | **Identify the documented information security policy** examined. |  | | | | | |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | | | | | | |
| * All relevant personnel. |  | | | | | |
| * All relevant vendors and business partners. |  | | | | | |
| **12.1.1** Review the security policy at least annually and update the policy when business objectives or the risk environment change. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1.1** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. | **Identify the document** reviewed to verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. |  | | | | | |
| **Describe how** the information security policy was verified to be: | | | | | | |
| * Reviewed at least annually. |  | | | | | |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  | | | | | |
| **12.2** Implement a risk assessment process, that:   * Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), * Identifies critical assets, threats, and vulnerabilities, and * Results in a formal, documented analysis of risk.   *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.2.a** Verify that an annual risk-assessment process is documented that:   * Identifies critical assets, threats, and vulnerabilities * Results in a formal, documented analysis of risk. | **Describe how** it was verified that an annual risk-assessment process is documented that: | | | | | | |
| * Identifies critical assets, threats and vulnerabilities. |  | | | | | |
| * Results in formal, documented analysis of risk. |  | | | | | |
| **12.2.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. | **Identify the risk assessment result documentation** reviewed to verify that:   * The risk assessment process is performed at least annually. * The risk assessment is performed upon significant changes to the environment. * The documented risk assessment process was followed. |  | | | | | |
| **12.3** Develop usage policies for critical technologies and define proper use of these technologies.  **Note:** Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.  Ensure these usage policies require the following: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3** Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed: | **Identify** critical technologies in use. |  | | | | | |
| **Identify the usage policies for all identified critical technologies** reviewed to verify the following policies (12.3.1-12.3.10) are defined:   * Explicit approval from authorized parties to use the technologies. * All technology use to be authenticated with user ID and password or other authentication item. * A list of all devices and personnel authorized to use the devices. * A method to accurately and readily determine owner, contact information, and purpose. * Acceptable uses for the technology. * Acceptable network locations for the technology. * A list of company-approved products. * Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. * Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. * Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **Identify the responsible** **personnel** interviewed who confirm usage policies for all identified critical technologies are implemented and followed (for 12.3.1–12.3.10):   * Explicit approval from authorized parties to use the technologies. * All technology use to be authenticated with user ID and password or other authentication item. * A list of all devices and personnel authorized to use the devices. * A method to accurately and readily determine owner, contact information, and purpose. * Acceptable uses for the technology. * Acceptable network locations for the technology. * A list of company-approved products. * Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. * Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. * Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **12.3.1** Explicit approval by authorized parties. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.1** Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies. | **Provide the name of the assessor** who attests that the usage policies were verified to include processes for explicit approval from authorized parties to use the technologies. |  | | | | | |
| **12.3.2** Authentication for use of the technology. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.2** Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token). | **Provide the name of the assessor** who attests that the usage policies were verified to include processes s for all technology used to be authenticated with user ID and password or other authentication item. |  | | | | | |
| **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 devices and personnel authorized to use the devices. | **Provide the name of the assessor** who attests that the usage policies were verified to include processes define a list of all devices and personnel authorized to use the devices. |  | | | | | |
| **12.3.4** A method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.4** Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). | **Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine:   * Owner * Contact Information * Purpose |  | | | | | |
| **12.3.5** Acceptable uses of the technology. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.5** Verify that the usage policies define acceptable uses for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  | | | | | |
| **12.3.6** Acceptable network locations for the technologies. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.6** Verify that the usage policies define acceptable network locations for the technology. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable network locations for the technology. |  | | | | | |
| **12.3.7** List of company-approved products. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.7** Verify that the usage policies include a list of company-approved products. | **Provide the name of the assessor** who attests that the usage policies were verified to include a list of company-approved products. |  | | | | | |
| **12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.8.a** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | **Provide the name of the assessor** who attests that the usage policies were verified to require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. |  | | | | | |
| **12.3.8.b** Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity. | **Describe how** configurations for remote access technologies were examined to verify that remote access sessions will be automatically disconnected after a specific period of inactivity. |  | | | | | |
| **Identify** any remote access technologies in use. |  | | | | | |
| **Identify** the period of inactivity specified. |  | | | | | |
| **12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | **Provide the name of the assessor** who attests that the usage policies were verified to require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. |  | | | | | |
| **12.3.10** For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. | **Provide the name of the assessor** who attests that the usage policies were verified to prohibit copying, moving or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  | | | | | |
| **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements. | **Provide the name of the assessor** who attests that the usage policies were verified to require, for personnel with proper authorization, the protection of cardholder data in accordance with PCI DSS Requirements. |  | | | | | |
| **12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.4.a** Verify that information security policy and procedures clearly define information security responsibilities for all personnel. | **Identify** **the information security policy and procedures** reviewed to verify that they clearly define information security responsibilities for all personnel. |  | | | | | |
| **12.4.b** Interview a sample of responsible personnel to verify they understand the security policies. | **Identify the responsible personnel** interviewed for this testing procedure who confirm they understand the security policy. |  | | | | | |
| **Provide the name of the assessor** who attests that the interviews of responsible personnel conducted verified that they understand the security policies. |  | | | | | |
| **12.5** Assign to an individual or team the following information security management responsibilities: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5** Examine information security policies and procedures to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: | **Identify** **the information security policies** reviewed to verify the specific and formal assignment of the following (including 12.5.1-12.5.5):   * Information security to a Chief Security Officer or other security-knowledgeable member of management. * Responsibility for establishing, documenting and distributing security policies and procedures. * Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel. * Establishing, documenting, and distributing security incident response and escalation procedures. * Administering user account and authentication management. * Monitoring and controlling all access to data. |  | | | | | |
| **12.5.1** Establish, document, and distribute security policies and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.1** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security policies and procedures. * Documenting security policies and procedures. * Distributing security policies and procedures. |  | | | | | |
| **12.5.2** Monitor and analyze security alerts and information, and distribute to appropriate personnel. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Monitoring and analyzing security alerts. * Distributing information to appropriate information security and business unit management personnel. |  | | | | | |
| **12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.3** Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Establishing security incident response and escalation procedures. * Documenting security incident response and escalation procedures. * Distributing security incident response and escalation procedures. |  | | | | | |
| **12.5.4** Administer user accounts, including additions, deletions, and modifications. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.4** Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for administering user account and authentication management. |  | | | | | |
| **12.5.5** Monitor and control all access to data. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned. | **Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for:   * Monitoring all access to data * Controlling all access to data |  | | | | | |
| **12.6** Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.a** Review the security awareness program to verify it provides awareness to all personnel about the importance of cardholder data security. | **Identify the documented security awareness program** reviewed to verify it provides awareness to all personnel about the importance of cardholder data security. |  | | | | | |
| **12.6.b** Examine security awareness program procedures and documentation and perform the following: | **Identify the documented security awareness program procedures and additional documentation** examined to verify that:   * The security awareness program provides multiple methods of communicating awareness and educating personnel. * Personnel attend security awareness training: * Upon hire, and * At least annually * Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy. |  | | | | | |
| **12.6.1** Educate personnel upon hire and at least annually.  ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.* | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). | **Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel. |  | | | | | |
| **12.6.1.b** Verify that personnel attend security awareness training upon hire and at least annually. | **Describe how** it was observed that all personnel attend security awareness training: | | | | | | |
| * Upon hire |  | | | | | |
| * At least annually |  | | | | | |
| **12.6.1.c** Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security. | **Identify the sample** of personnel interviewed who confirm they have completed security awareness training. |  | | | | | |
| For the interview, **summarize details of the interview** that verify their awareness of the importance of cardholder data security. |  | | | | | |
| **12.6.2** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy. | **Describe how** it was verified that, per the security awareness program, all personnel: | | | | | | |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  | | | | | |
| * Provide an acknowledgement at least annually. |  | | | | | |
| **12.7** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)  **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. | **Identify the documented policy** reviewed to verify requirement for background checks to be conducted:   * On potential personnel who will have access to cardholder data or the cardholder data environment. * Prior to hiring the personnel. |  | | | | | |
| **Identify the Human Resources personnel** interviewed who confirm background checks are conducted:   * On potential personnel who will have access to cardholder data or the cardholder data environment. * Prior to hiring the personnel. |  | | | | | |
| **Describe how** it was verified that background checks are conducted (within the constraints of local laws): | | | | | | |
| * On potential personnel who will have access to cardholder data or the cardholder data environment. |  | | | | | |
| * Prior to hiring the personnel. |  | | | | | |
| **12.8** Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8**Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data (for example, backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, those that receive data for fraud modeling purposes, etc.), as follows: | **Identify the documented policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data**, reviewed to verify policy defines the following from 12.8.1–12.8.5:   * Maintain a list of service providers. * Maintain a written agreement that includes an acknowledgement that the service providers will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer. * Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. * Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. * Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  | | | | | |
| **12.8.1** Maintain a list of service providers. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.1** Verify that a list of service providers is maintained. | **Describe how** the documented list of service providers was observed to be maintained (kept up-to-date). |  | | | | | |
| **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 CDE.  ***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. | **Describe how** written agreements for each service provider were observed to confirm they include an acknowledgement by service providers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer. |  | | | | | |
| **12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.3** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. | **Describe how** it was verified that the procedures for proper due diligence prior to engaging a service provider are implemented, as documented in the policies and procedures at 12.8. |  | | | | | |
| **12.8.4** Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.4** Verify that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. | **Describe how** it was verified that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. |  | | | | | |
| **12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.8.5** Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | **Describe how** it was observed that the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  | | | | | |
| **12.9 *Additional requirement for service providers only*:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.  **Note:** This requirement is a best practice until June 30, 2015, after which it becomes a requirement.  **Note:** The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.9 *Additional testing procedure for service provider assessments only****:*Review service provider’s policies and procedures and observe templates used for written agreement to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | **Indicate whether** the assessed entity is a service provider. **(yes/no)**  *If “no,” mark the remainder of 12.9 as “Not Applicable.”*  *If “yes”:* |  | | | | | |
| **Indicate whether** this ROC is being completed prior to June 30, 2015. **(yes/no)** |  | | | | | |
| *If “yes” AND the assessed entity does not have this in place ahead of the requirement’s effective date, mark the remainder of 12.9 as “Not Applicable.”*  *If “no” OR if the assessed entity has this in place ahead of the requirement’s effective date:* | | | | | | |
| **Identify the service provider’s policies and procedures** reviewed to verify that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  | | | | | |
| **Describe how** templates used for written agreement were observed to verify that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  | | | | | |
| **12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following: | **Identify** **the documented incident response plan and related procedures** examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows from 12.10.1–12.10.6:   * Create the incident response plan to be implemented in the event of system breach. * Test the plan at least annually. * Designate specific personnel to be available on a 24/7 basis to respond to alerts: * 24/7 incident monitoring * 24/7 incident response * Provide appropriate training to staff with security breach response responsibilities. * Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. * Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  | | | | | |
| **12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:   * Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage and responses of all critical system components. * Reference or inclusion of incident response procedures from the payment brands. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.1.a** Verify that the incident response plan includes:   * Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum. * Specific incident response procedures. * Business recovery and continuity procedures * Data back-up processes * Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). * Coverage and responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. * Communication strategies. * Requirement for notification of the payment brands. * Specific incident response procedures. * Business recovery and continuity procedures. * Data back-up processes. * Analysis of legal requirements for reporting compromises. * Coverage for all critical system components. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  | | | | | |
| **12.10.1.b** Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed. | **Identify the sample** of personnel interviewed who confirm that the documented incident response plan and procedures are followed. |  | | | | | |
| **Identify the sample** of previously reported incidents or alerts reviewed for this testing procedure. |  | | | | | |
| *For each item in the sample,* **describe how** documentation was reviewed to confirm that the documented incident response plan and procedures are followed. |  | | | | | |
| **12.10.2** Test the plan at least annually. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.2** Verify that the plan is tested at least annually. | **Describe how** it was observed that the incident response plan is tested at least annually. |  | | | | | |
| **12.10.3** Designate specific personnel to be available on a 24/7 basis to respond to alerts. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes. | **Identify** **the document** requiring 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **Identify the sample** **of responsible personnel** interviewed who confirm 24/7 incident response and monitoring coverage for:   * Any evidence of unauthorized activity. * Detection of unauthorized wireless access points. * Critical IDS alerts. * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **Describe how** it was observed that designated personnel are available for 24/7 incident response and monitoring coverage for: | | | | | | |
| * Any evidence of unauthorized activity. |  | | | | | |
| * Detection of unauthorized wireless access points. |  | | | | | |
| * Critical IDS alerts. |  | | | | | |
| * Reports of unauthorized critical system or content file changes. |  | | | | | |
| **12.10.4** Provide appropriate training to staff with security breach response responsibilities. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.4** Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained. | **Identify the sample of responsible personnel** interviewed who confirm that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **Identify the documented policy** reviewed that defines that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **Describe how** it was observed that staff with responsibilities for security breach response are periodically trained. |  | | | | | |
| **12.10.5** Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the Incident Response Plan. | **Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems are covered in the Incident Response Plan. |  | | | | | |
| **Describe how** processes were reviewed to verify that ***responding to*** alerts from security monitoring systems are covered in the Incident Response Plan. |  | | | | | |
| **12.10.6** Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.6** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  | | | | | |
| **Identify the sample of responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  | | | | | |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | | | | | | |
| * According to lessons learned. |  | | | | | |
| * To incorporate industry developments. |  | | | | | |