PCI Security Standards Council™

Payment Card Industry (PCI)
Data Security Standard

ROC Reporting Instructions
for PCI DSS v2.0

September 2011

Document Changes

Date	Document Version	Description	Pages
September 2011	1.0	To introduce PCI DSS ROC Reporting Instructions for PCI DSS version 2.0.	

Table of Contents

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures. The Report on Compliance (ROC) is produced during onsite PCI DSS assessments as part of an entity's validation process. The ROC provides details about the entity's environment and the assessment methodology, and documents the entity's compliance status for each PCI DSS Requirement.

The *PCI DSS Requirements and Security Assessment Procedures* includes a template for creating and completing a ROC. This document, *ROC Reporting Instructions*, provides additional instructions and guidance for assessors to ensure that a consistent level of reporting is maintained.

All details relevant to the assessor's findings should be clearly identified and documented in the appropriate place within the ROC. The information recorded in the ROC must ultimately support the assessor's findings of "in place" or "not in place" for each Requirement and Testing Procedure of the PCI DSS.

Report on Compliance Content

At a high level, the ROC provides a comprehensive summary of assessment activities performed and information collected during the assessment. The information contained in a ROC must provide enough detail and coverage to verify the entity's compliance status. The assessor should clearly describe how the validation activities were performed and how the resultant findings were reached for each section of the ROC.

As defined in the *PCI DSS Requirements and Security Assessment Procedures*, the ROC includes the following sections:

- Section 1: Executive Summary
- Section 2: Description of Scope of Work and Approach Taken
- Section 3: Details about Reviewed Environment
- Section 4: Contact Information and Report Date
- Section 5: Quarterly Scan Results
- Section 6: Findings and Observations
- Compensating Controls Worksheets (if applicable)

Sections 1-5 provide a detailed overview of the assessed environment and establish the framework for the assessor's findings. If these sections are not thoroughly and accurately completed, the assessment findings will not have proper context.

Section 6, "Findings and Observations", contains the assessor's findings for each Requirement and Testing Procedure of the PCI DSS as well as information that supports and justifies each finding. The information provided in the "Findings and Observations" summarizes how the testing procedures were performed and the findings achieved. This section includes all 12 PCI DSS requirements, as well as "Additional PCI DSS

Requirements for Shared Hosting Providers” (*Appendix A* in the PCI DSS). All findings and observations should be supported by and consistent with the information in Sections 1-5.

A completed Compensating Controls Worksheet must be included in the ROC for each compensating control used. Please refer to *PCI DSS Appendices B* and *C* for the Compensating Controls Worksheet template and instructions for completion.

Assessor Documentation

A PCI DSS compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment to support the assessor’s findings. The assessor’s work papers should be retained and protected in accordance with PCI SSC program requirements.

Not all the information in the work papers will be included in the ROC.   The ROC is effectively a summary of all the evidence collected, and while the information presented in the ROC is derived from the work papers, the ROC itself should not be a replication of every piece of evidence collected.

How to Use the ROC Reporting Instructions

These ROC Reporting Instructions identify the information and level of detail to be recorded in each section of the ROC.

Environment and Assessment Details (ROC Sections 1-6)

This section provides reporting instructions for all sections of the ROC, and is presented in two columns:

- **ROC Section** – Corresponds to the ROC template as provided in the “Instructions and Content for Report on Compliance” section of the *PCI DSS Requirements and Security Assessment Procedures*.
- **ROC Reporting Details** – Outlines the information and level of detail to be provided for each item in the ROC template.

Findings and Observations – PCI DSS Requirements (ROC Section 6)

This section contains instructions for reporting findings and observations for PCI DSS requirements, and is presented as follows:

- **PCI DSS Requirements and Security Assessment Procedures** – Corresponds to the Requirements and Testing Procedures of the PCI DSS.
- **ROC Reporting Details** – Outlines the information and level of detail to be provided for each testing procedure. Note that the format of responses in a ROC is not expected to mirror the format in the Reporting Details column. The information provided in the Reporting

Details column is bulleted and indexed in this document for ease of readability. It is not intended that assessors follow this format when writing a ROC. However, assessors should ensure that they include all the required information in each response.

- **Reporting Methodology** – Identifies which methods used by the assessor to collect the requisite evidence are to be reported in the ROC for each testing procedure. Note that the methods identified for inclusion in the ROC may not be all-inclusive of the methods used during an actual assessment. The assessor may need to perform additional methods during the assessment to reach a finding of “in place” or “not in place”. Where additional methods are used to validate a finding, the assessor should also report those details in the ROC.

Reporting Methodology

The reporting methodologies to be included for each testing procedure are identified with a check mark (✓) in the Reporting Methodology column. The different reporting methodologies are described in the following table.

Reporting Methodology	Description
Observe system settings, configurations	▪ Assessor observes actual system components ▪ May include different configuration files, settings, or other parameters on each system observed ▪ Observation may require assistance from appropriate personnel (e.g. administrator or support personnel) ▪ Observation verifies that such parameters are set to produce a specified outcome
Document reviews	▪ Assessor reviews documentation provided by the assessed entity ▪ Documentation may include but is not limited to: policies, procedures, processes, configuration standards, network diagrams, vendor documentation, reports, logs, audit trails, and industry standards and best practices ▪ Reviews of documentation verify the inclusion of items specified in the requirement/testing procedure
Interviews with personnel	▪ Assessor interviews person or persons as appropriate for the requirement/testing procedure ▪ Results of interviews may demonstrate that an action has or has not been performed, or that the interviewee has particular knowledge or understanding
Observe process, action, state	▪ Assessor observations may include, but are not limited to: • Actions of people performing or not performing a task or procedures • Behavior of system components in response to an action • Communications and network traffic • Environmental conditions, including physical controls • Walk-through of a process or procedure to verify the steps being performed • Other evidence or output resulting from a task or action ▪ Observation may require assistance from appropriate personnel ▪ Observation verifies a specified result or outcome
Identify sample	▪ Assessor selects a representative sample as appropriate for the requirement/testing procedure ▪ Justification of sample provides assurance that controls are uniformly and consistently applied to all business facilities and system components

ROC Reporting Details

Instructions provided in the Reporting Details column correspond with one or more checked columns in the Reporting Methodologies column, for each requirement/testing procedure. Guidance for understanding the instructions used in the Reporting Details column is provided below.

- **Example instruction: "Describe how system configurations…"**
  - Identify the files, parameters or settings which were examined (for example; boot configuration files, directory account permissions, access control lists, rule sets, connection setting, application access policy settings, startup configuration files, etc.) on each system component.
  - This is not intended to be a list of file names. However, the description should include a suitable amount of detail to provide assurance that the appropriate files were reviewed.
  - Generic phrases such as "system settings" or "system configurations" are not sufficient.
  - Describe how the observed files or settings satisfy the requirement/testing procedure.
- **Example instruction: "Identify the document …"**
  - Identify the reviewed document by name. *(**Note**: The term "document" may refer to multiple documents or documentation sets.)*
  - Ensure all identified documents are also included in the List of Documentation Reviewed, under "Details about Reviewed Environment" (Section 3).
  - Describe how the information contained within the reviewed document satisfies the requirement/testing procedure.
  - The assessor should confirm that processes, policies or procedures are in place and being followed, and not merely that a document exists.
  - By identifying a document in the ROC, the assessor is attesting that the processes, policies, procedures or practices contained in that document are sound.
- **Example instruction: "Identify the personnel interviewed…"**
  - Identify the roles or positions of the personnel interviewed.
  - If the testing procedure identifies personnel in a specific position to be interviewed, ensure that personnel in those positions are in fact interviewed.
  - If a specific position doesn't exist, it is the assessor's responsibility to identify the appropriate personnel to interview. Explain how interviews with the identified personnel meet the intent of the specified position.
  - Summarize the relevant details discussed during the interview and describe how the requirement/testing procedure is satisfied.
  - Ensure all interviewed persons are also included in the List of Individuals Interviewed, under "Details about Reviewed Environment" (Section 3).

- **Example instruction: "Describe how it was observed…"**
  - Identify and describe the process, procedure, action, or state that was observed.
  - Identify any personnel or system components that were part of the observation.
  - Describe any situational or environmental factors relevant to the observation.
  - Describe how the observations provide assurance that the requirement/testing procedure is satisfied.
- **Example instruction: "Identify all locations where…"**
  - Identify and briefly describe the number of applicable locations. If the entity under review has many locations that can be categorized into different location types, the assessor may simply identify and describe the different location types and number in each type.
- **Example instruction: "Identify all instances where…"**
  - Identify the circumstances applicable to the occurrence of a particular event.
- **Example instruction: "Identify the sample of…"**
  - Identify the number and type of items included in each sample (for example; 2 of the 4 perimeter routers at head office, manager workstations from 10 of 60 standard retail outlets, application servers 001 and 002, etc.).
  - It is not necessary to identify the names of every sampled system component in the ROC. However, assessors may provide a list if it improves clarity or better explains the findings for some environments. Irrespective of whether system component names are recorded in the ROC, the assessor must maintain a detailed record of each sampled component in their work papers, and provide full details of the sampling methodology in the "Description of Scope of Work and Approach Taken" section of the ROC.
  - The samples identified in the "Findings and Observations" must correspond with the information provided in the "Description of Scope of Work and Approach Taken," where full details of the sampling methodology and justification for sampling selections is to be thoroughly documented.
  - Samples must be representative of the entire environment and cover all business facilities and system components.
  - The types of business facilities and/or system components in the sample must be appropriate for the requirement/testing procedure.

Compensating Controls, Not Applicable, and Future-Dated Requirements

If a PCI DSS Requirement or Testing Procedure is deemed to be in place due to the implementation of compensating controls, or because it was determined to be "not applicable" (N/A), this should be clearly identified in the "In Place" column. Findings of "in place" due to being N/A must include details of how the Requirement or Testing Procedure was verified to be not applicable. Findings of "in place" due to compensating controls must be accompanied by a completed Compensating Controls Worksheet in the ROC appendices.

For future-dated requirements (for example, the ranking of newly identified vulnerabilities defined in Testing Procedure 6.2.a), record in the "In Place" column whether the requirement was observed to be implemented and any observations that support this finding. If the requirement is not implemented prior to its effective date it should be noted as such; however, it should not impact the overall compliance finding of the assessment.

Do's and Don'ts: General Guidance and Best Practices

DO:

- Follow the ROC template provided in the *PCI DSS Requirements and Security Assessment Procedures*.
- Complete all sections in the order specified, with consistent numbering, titles, and headings.
- Read and understand the intent of each Requirement and Testing Procedure.
- Provide a response for every Testing Procedure.
- Provide sufficient detail and information to demonstrate a finding of "in place".
- Describe how a Requirement was verified, not just that it was verified.
- Describe what was performed for each Testing Procedure.
- Ensure the response addresses all parts of the Testing Procedure.
- Ensure the response covers all applicable system components.
- Ensure the lists of documentation, interviewees, hardware and critical software in the "*Details About Reviewed Environment"* section are complete and include all such items referenced in the body of the ROC.
- Complete a Compensating Controls Worksheet for each and every compensating control.
- Perform an internal quality assurance review of the ROC for clarity, accuracy, and quality.

DON'T:

- Don't report items in the "In Place" column unless they have been verified as being "in place".
- Don't include forward-looking statements or project plans in the "In Place" column.
- Don't repeat or echo the Testing Procedure in the response.
- Don't copy responses from one Testing Procedure to another.
- Don't copy responses from previous assessments.
- Don't cross-reference between responses.
- Don't include information that is not relevant to the assessment or individual findings.

ROC Reporting Instructions for PCI DSS v2.0

Environment and Assessment Details (ROC Sections 1-6)

ROC Section *(PCI DSS template)*	ROC Reporting Details
1. Executive Summary	
▪ Describe the entity's payment card business, including:	• Provide an overview of the entity's role with payment cards.
– Their business role with payment cards, which is how and why they store, process, and/or transmit cardholder data ***Note:*** *This is not intended to be a cut-and-paste from the entity's web site, but should be a tailored description that shows the assessor understands payment and the entity's role.*	• Describe the entity's business role with payment cards, including: ○ How the entity stores, processes and/or transmits cardholder data ○ Why the entity stores, processes and/or transmits cardholder data
– How they process payment (directly, indirectly, etc.)	• Describe how payments are processed including whether they are processed directly or indirectly.
– What types of payment channels they serve, such as card-not-present (for example, mail order/telephone order (MOTO), e-Commerce), or card-present	• Identify and describe all payment channels in use, including whether they are card-present or card-not-present.
– Any entities that they connect to for payment transmission or processing, including processor relationships	• Provide a list of all parties that the assessed entity connects to for: ○ Payment transmission ○ Payment processing • Provide a brief description of the purpose for each connection.
▪ A high-level network diagram (either obtained from the entity or created by assessor) of the entity's networking topography that includes:	• Provide one or more simple, high-level diagrams(s) showing the overall architecture of the environment being assessed. The diagrams should identify all locations and key systems, and the boundaries between them. • Ensure the diagram(s) includes the following:
– Connections into and out of the network	○ All connections into and out of the network, including demarcation points between the cardholder data environment (CDE) and other networks/zones
– Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable	○ All critical components and key systems, as well as their locations and the boundaries between them
– Other necessary payment components, as applicable	○ All other necessary components or key systems, their locations and boundaries, as applicable

ROC Section *(PCI DSS template)*	ROC Reporting Details
2. Description of Scope of Work and Approach Taken	
▪ Document how the assessor validated the accuracy of the PCI DSS scope for the assessment, including:	• Describe how the assessor validated the accuracy of the PCI DSS scope for the assessment, including the following:
– The methods or processes used to identify and document all existences of cardholder data	○ Describe the methods or processes (for example, tools, observations, feedback, scans, data flow analysis, etc.) that the entity used to: – Identify and document all existences of cardholder data – Verify that no cardholder data exists outside of the CDE scope defined for this assessment.
– How the results were evaluated and documented	○ Describe how the results of the methods/processes were: – Evaluated to verify that PCI DSS scope is appropriate – Documented (for example, the results may be a diagram or an inventory of cardholder data locations)
– How the effectiveness and accuracy of the methods used were verified	○ Explain why the methods used for scope verification are considered by the assessor to be effective and accurate.
– That the assessor validates that the scope of the assessment is accurate and appropriate.	○ Provide a statement that the assessor confirms that the scope of the assessment is accurate and appropriate.
▪ Environment on which the assessment focused (for example, client's Internet access points, internal corporate network, processing connections)	• Provide an overview of the scope of this assessment encompassing the people, processes, technologies, and locations. *Examples include but are not limited to:* ○ *People* – such as technical support, management, administrators, operations teams, cashiers, telephone operators, etc. ○ *Processes* – such as payment channels, business functions, etc. ○ *Technologies* – such as e-commerce systems, internal network segments, DMZ segments, processor connections, POS systems, etc. ○ *Locations/sites/stores* – such as retail outlets, data centers, corporate office locations, call centers, etc.

ROC Section *(PCI DSS template)*	**ROC Reporting Details**
▪ If network segmentation is in place and was used to reduce the scope of the PCI DSS review, briefly explain that segmentation and how assessor validated the effectiveness of the segmentation.	• Identify whether the assessed entity has used network segmentation to reduce the scope of the assessment.
	• ***If segmentation is not used:*** Provide a statement that the assessor confirms that the whole network has been included in the scope of the assessment.
	• ***If segmentation is used:*** Briefly describe how the segmentation is implemented, as follows; ○ Identify the technologies used and any supporting processes ○ Identify all network segments (both in-scope and out of scope) ○ For each network segment: – Provide a brief description of the function/purpose of the segment – Identify whether the segment is a wireless or wired network – Identify whether the segment is in scope for the assessment: ▪ Identify segments that store, process or transmit cardholder data (CDE segment) ▪ Identify segments that don't store, process or transmit cardholder data, but that: ○ Have connectivity to the CDE, and/or ○ Allow controlled access into the CDE – Wherever access is permitted from a non-CDE segment into a CDE segment: ▪ Identify what access is permitted and for what purpose ▪ Describe how the access is controlled/ restricted/ managed ○ Explain how the assessor validated the effectiveness of the segmentation, as follows; – Describe the methods used to validate the effectiveness of the segmentation (for example, observed configurations of implemented technologies, tools used, network traffic analysis, etc.) – Describe how it was verified that: ▪ The segmentation is functioning as intended ▪ Adequate security controls are in place to ensure the integrity of the segmentation mechanisms (e.g., access controls, change management, logging, monitoring, etc.) ○ Confirm that the technologies/processes used to implement segmentation were included in the scope of the PCI DSS assessment ○ Provide a statement that the assessor confirms the segmentation is adequate to reduce the scope of the assessment.

ROC Section *(PCI DSS template)*	ROC Reporting Details
▪ If sampling is used during the assessment, for each sample set selected (of business facilities/system components) document the following:	• Identify whether sampling was used during the assessment
	• ***If sampling was not used:*** Provide a statement that the assessor confirms that every system component and all business facilities have been assessed.
	• ***If sampling was used:*** ○ List all sample sets used (for example, firewalls, application servers, retail locations, data centers, User IDs, people, etc.).
– Total population	○ For each sample set: – Identify the size of the total population.
– Number sampled	– Identify the number of items in each sample.
– Rationale for sample selected	– What was considered when selecting the size of the sample. – What was considered when selecting the items to include in the sample.
– Description of the standardized PCI DSS security and operational processes and controls used to determine sample size, and how the processes/controls were validated	– Identify whether any standardized security and operational processes and controls are in place in the environment, which were relied on to determine sample sizes. ▪ If yes, explain how the assessor verified that the standardized processes/controls ensure consistency and apply to all items in the population.
– How the sample is appropriate and representative of the overall population	– Explain why the selected sample: ▪ Is representative of the overall population ▪ Is large enough to provide the assessor with assurance and confidence that the same conclusion would have been reached had the entire population been reviewed
▪ Description of any locations or environments that store, process, or transmit cardholder data that were EXCLUDED from the scope of the review, and why these locations/environments were excluded.	• Identify and describe any locations or environments which were excluded from the assessment. • Explain why they were excluded.
▪ List any wholly-owned entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment.	• List all wholly-owned entities (this may include subsidiaries, different brands, DBAs, etc.) that the assessed entity owns that are required to comply with PCI DSS. • For each wholly-owned entity, explain whether they have been reviewed as part of this assessment or they are reviewed separately.
▪ List any international entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment.	• List all countries where the entity conducts business. • If the assessed entity operates in other countries, identify all international operations that are required to comply with PCI DSS. • For each international operation required to comply with PCI DSS, explain whether they have been reviewed as part of this assessment or they are reviewed separately.

ROC Section *(PCI DSS template)*	ROC Reporting Details
▪ List any wireless LANs and/or wireless payment applications (for example, POS terminals) that are connected to or could impact the security of the cardholder data environment, and describe security in place for these wireless environments.	• Identify and describe all wireless technologies in use. This would include: o Wireless LANs o Wireless payment applications (for example, POS terminals) o All other wireless devices/technologies • If there are no wireless networks or technologies in use, describe how this was verified by the assessor.
	• For each wireless technology that exists: o Identify if the technology is in scope for the assessment. o For each wireless technology in scope, identify the following: – Whether the technology is used to store, process, or transmit cardholder data – Whether the technology is connected to or part of the CDE – Whether the technology could impact the security of the cardholder data environment o Describe the security in place for each wireless technology in scope. o For each wireless technology determined as not in scope for this assessment, describe how this was verified by the assessor.
▪ Identify the version of the PCI DSS Requirements and Security Assessment Procedures document used to conduct the assessment.	• State the version number of the *PCI DSS Requirements and Security Assessment Procedures* that was used to conduct the assessment.
3. Details about Reviewed Environment	
Include the following details in this section: ▪ A diagram of each piece of the communication link, including LAN, WAN, or Internet	• Identify each communication/connection point in scope. • Provide one or more detailed diagrams to illustrate each communication point. Diagrams should include the following: o All boundaries of the cardholder data environment o Any network segmentation points which are used to reduce scope of the assessment o Boundaries between trusted and untrusted networks o Wireless and wired networks o All other connection points applicable to the assessment • Ensure the diagram(s) include enough detail to clearly understand how each communication point functions and is secured. (For example, the level of detail may include identifying the types of devices, device interfaces, network technologies, protocols, and security controls applicable to that communication point.) ***Note:*** *This diagram or diagrams are additional to the high-level diagram provided in Section 1 and should provide a more detailed view of the communication points within the environment.*

ROC Section *(PCI DSS template)*	ROC Reporting Details
▪ Description of cardholder data environment, for example: – Document transmission and processing of cardholder data, including authorization, capture, settlement, chargeback, and other flows as applicable	• Provide a detailed description of cardholder data environment, including the following. ○ Identify all transmission and processing flows of cardholder data, including: – Authorization – Capture – Settlement – Chargeback – Any other flows as applicable ○ For each transmission and processing flow: – Describe how cardholder data is transmitted and/or processed. – Identify the types of cardholder data involved (for example, full track, PAN, expiry date). ***Note:*** *Include all types of data flows, including any involving hard-copy/paper media. A combination of descriptions and data-flow diagrams may be helpful to illustrate this.*
– List of files and tables that store cardholder data, supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers. This inventory should include, for each cardholder data store (file, table, etc.):	• Identify and list all databases, tables, and files storing cardholder data (including electronic and hard copy). • For each item in the list, provide the following information:
• List all of the elements of stored cardholder data	○ All elements of cardholder data stored, e.g., PAN, expiry date
• How data is secured	○ A description of the security controls in place for protection of the data (for example, use of encryption, access controls, truncation, etc.)
• How access to data stores are logged	○ A description of the logging mechanisms used for logging access to data (for example, enterprise log management solution, application-level logging, operating system logging, etc.)

ROC Section *(PCI DSS template)*	ROC Reporting Details
• List of hardware and critical software in use in the cardholder data environment, along with description of function/use for each	• Identify and list all types of hardware in the cardholder data environment, including but not limited to: ○ Network components ○ Servers and other systems (mainframes, mid-range, etc.) ○ Devices performing security functions ○ End-user devices (such as laptops and workstations) ○ Virtualized devices • For each item in the list, provide: ○ The type of device and vendor (make and model, as applicable) ○ A description of the function/purpose of the device
	• Identify and list all critical software in the cardholder data environment, including but not limited to: ○ All software involved in storing, processing, or transmitting CHD, for example: – Payment applications (both commercial and custom) – Databases and other software storage products – VPN and gateway software ○ E-commerce applications ○ Applications accessing cardholder data for non-payment functions (for example, fraud modeling, credit verification, etc.) ○ Software performing security functions or enforcing PCI DSS controls (for example, two-factor authentication solution, access control servers, certificate servers, anti-virus programs, patching software, firewall or IDS software, logging solutions, etc.) ○ Underlying operating systems for systems that store, process, or transmit CHD ○ System management software (for example, remote management utilities, configuration management tools, etc.) ○ Virtualization management software • For each item in the list, provide: ○ The type of software and vendor (software name and version, as applicable) ○ A description of the function/purpose of the software
▪ List of service providers and other third parties with which the entity shares cardholder data (Note: These entities are subject to PCI DSS Requirement 12.8.)	• Identify and list all service providers and other third parties with which the entity shares cardholder data. • For each service provider or third party, provide: ○ Company name ○ What data is shared (for example, PAN, expiry date, etc.) ○ The purpose for sharing the data (for example, third-party storage, transaction processing, etc.)

ROC Section *(PCI DSS template)*	ROC Reporting Details
▪ List of third-party payment application products and versions numbers in use, including whether each payment application has been validated according to PA-DSS. Even if a payment application has been PA-DSS validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's PA-DSS Implementation Guide. ***(Note:** It is not a PCI DSS requirement to use PA-DSS validated applications. Please consult with each payment brand individually to understand their PA-DSS compliance requirements.)*	• Identify and list all third-party payment applications. Include the following: ○ Name of product ○ Version of product ○ Whether each payment application has been validated according to PA-DSS ○ PA-DSS reference number, if applicable ○ Expiry date of PA-DSS validation, if applicable • Provide a statement that the assessor confirms that all PA-DSS validated payment applications were reviewed to verify they have been implemented in a PCI DSS compliant manner according to the payment application vendor's PA-DSS Implementation Guide.
▪ List of individuals interviewed, their organization, titles, and topics covered	• Identify and list the individuals interviewed. Include the following: ○ The individual's name ○ The individual's organization ○ The individual's job title ○ A summary of the topics covered
▪ List of documentation reviewed	• Identify and list all reviewed documents. Include the following: ○ Document name ○ Brief description of document purpose ○ Document date
▪ For managed service provider (MSP) reviews, the assessor must clearly identify which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans.	• State whether the entity being assessed is a managed service provider • If the entity is a managed service provider: ○ List the requirements which apply to the MSP and are included in this assessment. ○ List the requirements which are the responsibility of the MSP's customers (and have not been included in this assessment). ○ Identify which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans. ○ Identify which of the MSP's IP addresses are the responsibility of the MSP's customers.

ROC Section *(PCI DSS template)*	ROC Reporting Details
4. Contact Information and Report Date	
▪ Contact information for merchant or service provider and assessor	• Provide the following information for both the entity being assessed and the assessor: ○ Contact name ○ E-mail address ○ Company name ○ Company address
▪ Timeframe of assessment – Specify the duration and the time period over which the assessment occurred.	• Provide the following details about the timeframe of the assessment: ○ Time Period – The total time taken to complete the overall assessment (start date to completion date). ○ Duration – Description of how much time during the overall Time Period was spent on the assessment. Include time spent onsite at the entity or performing remote assessment activities, and validation of remediation activities.
▪ Date of report	• Provide the date this report was completed.

ROC Section *(PCI DSS template)*	ROC Reporting Details
5. Quarterly Scan Results	
▪ Summarize the four most recent quarterly ASV scan results in the Executive Summary as well as in comments at Requirement 11.2.2. **Note:** *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies:* – *The most recent scan result was a passing scan,* – *The entity has documented policies and procedures requiring quarterly scanning going forward, and* – *Any vulnerabilities noted in the initial scan have been corrected as shown in a re-scan.* – *For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*	• Identify whether this is the assessed entity's initial PCI DSS compliance validation.
	• ***If this is <u>not</u> the entity's initial PCI DSS assessment:*** ○ Identify the four external quarterly ASV scans performed within the last 12 months. ○ For each of the four quarterly ASV scans performed within the last 12 months, identify; – Dates of the scans – Results of scans – Pass or Fail – For all scans resulting in a Fail, provide the re-scan date(s).
	• ***If this is the entity's initial PCI DSS assessment:*** ○ Identify how many external quarterly ASV scans were performed within the last 12 months. ○ Identify that the most recent scan result is a passing scan. ○ Identify the entity's documented policies and procedures which require quarterly ASV scans going forward. ○ For each quarterly ASV scan performed within the last 12 months, identify: – Dates of the scan(s) – Whether any vulnerabilities were found, resulting in a failed initial scan – For all scans resulting in a Fail, provide date(s) of re-scans showing that the vulnerabilities have been corrected.
▪ Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the *PCI Approved Scanning Vendors (ASV) Program Guide.*	• Provide a statement that the assessor has verified that the ASV and the entity have completed the Attestations of Scan Compliance confirming that all externally accessible (Internet-facing) IP addresses in existence at the entity were appropriately scoped for the ASV scans.

ROC Section *(PCI DSS template)*	ROC Reporting Details
6. Findings and Observations	
▪ Summarize in the Executive Summary any findings that may not fit into the standard Report on Compliance template format.	• Identify any findings that the assessor feels are relevant to assessment findings, but that do not fall under a PCI DSS requirement.
All assessors *must:*	
▪ Use the detailed *PCI DSS Requirements and Security Assessment Procedures* template to provide detailed report descriptions and findings on each requirement and sub-requirement.	• Ensure that the correct ROC template is used for the version of PCI DSS that the assessment was based on. • Ensure that the ROC template defined in the *PCI DSS Requirements and Security Assessment Procedures* is followed, including: ○ Sections should be presented in the same order as the ROC template. ○ Section numbering should be consistent with the ROC template. ○ Section and table headings should be consistent with the ROC template.
▪ Ensure that all N/A responses are clearly explained.	• If a requirement is deemed to be "in place" due to N/A, document as such in the "In Place" column, and provide details of how the requirement was verified as being N/A. The details may be recorded in the "Notes" column for the requirement, or in a table format (in an appendix) if there are too many details to fit in the "Notes" column of the requirement. *Note:* The assessor may include a list of the requirements determined to be N/A and a brief justification for each in the 'Description of Scope of Work and Approach Taken' section. This may be useful if there are a large number of N/A responses, or there is significant impact on how the assessment was performed.
▪ Review and document any compensating controls considered to conclude that a control is in place. *See "Compensating Controls" section above and* Appendices B *and* C *for more details on compensating controls.*	• Confirm that a Compensating Controls Worksheet has been completed for each compensating control identified. • Include all Compensating Controls Worksheets in an appendix, with a uniquely identifying appendix number for each. (For example, if Compensating Controls Worksheets are in Appendix B of the ROC, uniquely identify each worksheet as B-1, B-2, etc.) • Wherever a compensating control is used to meet a PCI DSS requirement, document as such in the "In Place" column, and clearly identify where the worksheet for that compensating control is located in the appendix. • Ensure that the all Compensating Controls Worksheets follow the defined template in Appendix C of the *PCI DSS Requirements and Security Assessment Procedures*. *Note:* The assessor may include a list of the compensating controls together with a brief description and the affected requirements, at the beginning of the Appendix where the Compensating Controls Worksheets are located. This may be useful if there are a large number of requirements affected by compensating controls, or there is significant impact on how the assessment was performed.

Findings and Observations – PCI DSS Requirements (ROC Section 6)

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 1: Install and maintain a firewall configuration to protect cardholder data							
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:						
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	• Identify the document(s) which defines the formal processes for: i. Testing of all network connections ii. Approval of all network connections iii. Testing of all firewall configuration changes iv. Approval of all firewall configuration changes v. Testing of all router configuration changes vi. Approval of all router configuration changes • Describe how the documented processes were observed to be implemented, for: i. Testing of all network connections ii. Approval of all network connections iii. Testing of all firewall configuration changes iv. Approval of all firewall configuration changes v. Testing of all router configuration changes vi. Approval of all router configuration changes		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.	• Identify the current network diagram(s). • Describe how observed network connections confirm that the diagram: i. Is current ii. Includes all connections to cardholder data iii. Includes any wireless network connections		✓		✓	
	1.1.2.b Verify that the diagram is kept current.	• Identify the document requiring that the network diagram is kept current. • Describe the documented process for keeping the network diagram current. • Identify the responsible personnel interviewed who confirm the documented process is followed.		✓	✓		
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3.a** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	• Identify the firewall configuration standards that define requirements for: i. A firewall at each Internet connection ii. A firewall between any DMZ and the internal network zone		✓			
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.	• Identify the current network diagrams and firewall configuration standards reviewed. • Describe how the reviewed documents were confirmed to be consistent with one another.		✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.	• Identify the firewall configuration standards that include descriptions of the following for logical management of components: i. Groups ii. Roles iii. Responsibilities • Identify the router configuration standards that include descriptions of the following for logical management of components: i. Groups ii. Roles iii. Responsibilities • Identify the personnel holding those roles and responsibilities who were interviewed, and who confirm that the roles and responsibilities are assigned as documented for: i. Logical management of router components ii. Logical management of firewall components		✓	✓		
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.	**1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.	• For each of the following, identify the firewall configuration standards which define those necessary for business, including a business justification for each: i. Services ii. Protocols iii. Ports • For each of the following, identify the router configuration standards which define those necessary for business, including a business justification for each: i. Services ii. Protocols iii. Ports		✓			

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.	• Identify whether any insecure services, protocols or ports are allowed. • For each insecure service, protocol and port allowed: i. Identify the documented justification. ii. Identify the responsible personnel interviewed who confirm that each insecure service/protocol/port is necessary. iii. Identify the firewall and router configuration standards which define the security features required for each insecure service/protocol/port. iv. Describe how observed firewall configurations verify the security features are implemented. v. Describe how observed router configurations verify the security features are implemented.	✓	✓	✓		
1.1.6 Requirement to review firewall and router rule sets at least every six months	**1.1.6.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	• Identify the firewall configuration standards that require a review of firewall rule sets at least every six months. • Identify the router configuration standards that require a review of router rule sets at least every six months.		✓			
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.	• Identify documented results of previous: i. Firewall rule set reviews ii. Router rule set reviews • Identify the responsible personnel interviewed who confirm that: i. Firewall rule set reviews are completed at least every six months. ii. Router rule set reviews are completed at least every six months.		✓	✓		

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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 to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:						
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	**1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.	• Describe how observed firewall/router configurations limit traffic to that which is necessary for the cardholder data environment: i. Inbound ii. Outbound • Identify the document that defines the restrictions and confirm this is consistent with the observed configurations: i. Inbound ii. Outbound • Describe how inbound and outbound traffic was observed to be limited to that which is necessary for the cardholder data environment: i. Inbound ii. Outbound	✓	✓		✓	
	1.2.1.b 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 observed to specifically deny all other traffic: i. Inbound ii. Outbound	✓				

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
1.2.2 Secure and synchronize router configuration files.	**1.2.2** Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.	• Describe how the router configuration files were observed to be secured • Describe how the router configuration files were observed to be synchronized.	✓			✓	
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	**1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	• Describe how firewalls were observed to be in place between any wireless networks and systems that store cardholder data. • Describe how firewall configurations were observed to deny or control all traffic from any wireless environment into the cardholder data environment. • Identify the responsible personnel interviewed who confirm that any permitted traffic from the wireless environment into the cardholder data environment is necessary for business purposes.	✓		✓	✓	
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—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment, as detailed below.						
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** Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	• Identify the document defining system components that provide authorized publicly accessible services, protocols, and ports. • Describe how observed firewall/router configurations ensure that the DMZ limits inbound traffic to only those system components.	✓	✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Verify that inbound Internet traffic is limited to IP addresses within the DMZ.	• Describe how observed firewall/router configurations limit inbound Internet traffic to IP addresses within the DMZ. • Describe how inbound Internet traffic was observed to be limited 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** Verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.	• Identify the network documents/diagrams specifying that direct connections are not allowed for traffic between the Internet and the cardholder data environment: i. Inbound ii. Outbound • Describe how observed firewall/router configurations prevent direct connections between the Internet and the cardholder data environment: i. Inbound ii. Outbound • Describe how observed traffic between the Internet and the cardholder data environment confirms that direct connections are not permitted: i. Inbound ii. Outbound	✓	✓		✓	
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	**1.3.4** Verify that internal addresses cannot pass from the Internet into the DMZ**.**	• Describe how observed firewall/router configurations prevent internal addresses passing from the Internet into the DMZ. • Describe how observed traffic from the Internet into the DMZ confirms that internal addresses cannot pass from the Internet into the DMZ.	✓			✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.5** Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized	• Identify the document that explicitly defines authorized outbound traffic from the cardholder data environment to the Internet. • Describe how firewall/router configurations were observed to allow only explicitly authorized traffic. • Describe how observed outbound traffic from the cardholder data environment to the Internet confirms that only explicitly authorized traffic is allowed.	✓	✓		✓	
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** 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 observed firewall configurations implement stateful inspection. • Describe how observed network traffic confirms that stateful inspection is implemented (that is, only "established" connections are allowed into the network).	✓			✓	
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**1.3.7** Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	• For all system components that store cardholder data: i. Identify the diagrams and/or other document(s) which define how system components are located on an internal network zone, segregated from the DMZ and other untrusted networks. ii. Describe how observed network and system configurations confirm the system components are located on an internal network zone, segregated from the DMZ and other untrusted networks. iii. Describe how observed network traffic confirms that the system components are located on an internal network zone, segregated from the DMZ and other untrusted networks.	✓	✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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 or content caches,* • *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** Verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	• Identify the document defining methods to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. • Briefly describe the methods in place. • Describe how observed firewall/router configurations prevent private IP addresses and routing information from being disclosed to the Internet. • Describe how observed network traffic confirms that private IP addresses and routing information are not disclosed to the Internet.	✓	✓		✓	
	1.3.8.b Verify that any disclosure of private IP addresses and routing information to external entities is authorized.	• Identify the document 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. • Describe how observed configurations ensure that any disclosure of private IP addresses and routing information to external entities is authorized.	✓	✓	✓		

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	**1.4.a** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.	• Identify whether mobile and/or employee-owned computers with direct connectivity to the Internet are used to access the organization's network. • Identify the document requiring that mobile and/or employee-owned computers with direct connectivity to the Internet have personal firewall software: i. Installed ii. Active • Describe how personal firewall software was observed on mobile and/or employee-owned computers to be: i. Installed ii. Active	✓	✓		✓	
	1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by users of mobile and/or employee-owned computers.	• Identify the document defining personal firewall software configuration standards. • Describe how personal firewall software on mobile and/or employee-owned computers was observed to be: i. Configured by the organization to the documented configuration standards ii. Not alterable by mobile and/or employee-owned computer users	✓	✓			
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters							
2.1 Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	**2.1** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	• Identify the sample of system components observed. • For each sampled system component, describe how attempts to log on using vendor-supplied accounts and passwords confirm that all default accounts and passwords are changed before installing a system on the network.				✓	✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2.1.1** Verify the following regarding vendor default settings for wireless environments:						
	2.1.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions	• Identify the document requiring that wireless encryption keys must be changed: i. From default at installation ii. Anytime anyone with knowledge of the keys leaves the organization or changes positions • Identify the responsible personnel interviewed who confirm the documented processes for changing keys are followed: i. At installation ii. Anytime anyone with knowledge of the keys leaves the organization or changes positions • Describe how observed wireless configurations confirm that key changes are completed as required.	✓	✓	✓		
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.	• Identify the document requiring that default SNMP community strings must be changed. • Describe how observed wireless configurations confirm that default SNMP community strings are changed.	✓	✓			
	2.1.1.c Verify default passwords/passphrases on access points were changed.	• Identify the document requiring that default passwords/passphrases on access points must be changed. • Describe how observed wireless configurations confirm that default passwords/passphrases are changed.	✓	✓			
	2.1.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.	• Identify the document requiring that firmware on wireless devices must be updated to support strong encryption for: i. Authentication ii. Transmission • Describe how observed wireless configurations confirm that firmware is updated to support strong encryption for: i. Authentication ii. Transmission	✓	✓			

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	2.1.1.e Verify other security-related wireless vendor defaults were changed, if applicable.	• Identify the document that defines any other security-related wireless vendor defaults. • Describe how the observed wireless configurations confirm that other security-related vendor defaults are changed, as 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 • Describe how the configuration standards were confirmed to: i. Cover all types of system components ii. Address all known security vulnerabilities iii. Be consistent with industry-accepted system hardening standards • Identify the industry-accepted hardening standards.		✓			
	2.2.b Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.	• Describe the process for updating system configuration standards as new vulnerability issues are identified. • Identify the responsible personnel interviewed who confirm that the process is followed. • Describe how the process was observed to be implemented. • Describe how the reviewed system configuration standards were confirmed to be updated with new vulnerability issues.		✓	✓	✓	
	2.2.c Verify that system configuration standards are applied when new systems are configured.	• Identify the document defining the process for applying system configuration standards to new systems. • Describe how observed system configurations confirm the configuration standards are applied. • Describe how it was observed that configuration standards are applied when new systems are configured.	✓	✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	2.2.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).	• Identify the system configuration standards requiring that: i. Only one primary function is implemented per server, including virtual system components or devices, as applicable. ii. Only necessary services or protocols are enabled and security features are implemented for any required services, protocols or daemons considered insecure. iii. System security parameters are configured to prevent misuse. iv. All unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.		✓			
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** For a sample of system components, verify that only one primary function is implemented per server.	• Identify the sample of system components observed. • For each sampled system component, describe how observed system configurations confirm that only one primary function per server is implemented.	✓				✓
	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.	• Identify personnel interviewed and describe how systems were observed to determine whether virtualization technologies are used. • If virtualization technologies are used: i. Identify the functions for which virtualization technologies are used. ii. Identify the sample of virtual system components or devices observed. iii. For each sampled virtual system component and device, describe how the observed configurations confirm only one primary function is implemented per virtual system component or device.	✓		✓	✓	✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	**2.2.2.a** For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled.	• Identify the sample of system components observed. • For each sampled system component: i. Describe how system configurations were inspected to identify all enabled: ○ Services ○ Daemons ○ Protocols ii. Identify the document specifying that each enabled service, daemon and protocol is necessary for that system component.	✓	✓			✓
	2.2.2.b Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented.	• From the sample of system components observed in 2.2.2.a, identify if any insecure services, daemons, or protocols are enabled. • For each insecure service, daemon, or protocol identified: i. Briefly describe why it is considered to be insecure. ii. Identify the documented business justification. iii. Identify the document defining security features for the insecure service, daemon or protocol. iv. Describe how the observed system configurations confirm that security features are implemented in accordance with documentation.	✓	✓		✓	
2.2.3 Configure system security parameters to prevent misuse.	**2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.	• Identify the systems administrators, security managers and other responsible personnel interviewed. • Describe how each person interviewed demonstrated they have knowledge of common security parameter settings for the system components that they configure.			✓		
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.	• Identify the system configuration standards that define the common security parameter settings.		✓			
	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.	• Identify the sample of system components observed. • For each sampled system component, describe how common security parameters were observed to be set according to the documented system configuration standards.	✓				✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4.a** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	• Identify the sample of system components observed. • For each sampled system component, describe how it was observed that all unnecessary functionality is removed.	✓			✓	✓
	2.2.4.b. Verify enabled functions are documented and support secure configuration.	• For each sampled system component: i. Identify the document defining the authorized functions that are allowed to be enabled. ii. Describe how enabled functions were identified on each system component. iii. Confirm that all observed enabled functions are documented. iv. Describe how the enabled functions were observed to support secure configuration.	✓	✓			
	2.2.4.c. Verify that only documented functionality is present on the sampled system components.	• For each sampled system component, describe how documentation and observed system configurations were compared to confirm that only documented functionality is present on the system components.	✓	✓			
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**2.3** For a sample of system components, verify that non-console administrative access is encrypted by performing the following:						
	2.3.a Observe an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested.	• Identify the sample of system components observed • For each sampled system component: i. Identify the strong encryption method used for non-console administrative access. ii. Describe how strong encryption was observed to be invoked before the administrator password is requested.				✓	✓
	2.3.b Review services and parameter files on systems to determine that Telnet and other remote login commands are not available for use internally.	• For each sampled system component, describe how the observed services and parameter files confirm that the following are not available for use internally: i. Telnet ii. Other remote log-in commands	✓				

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	2.3.c Verify that administrator access to the web-based management interfaces is encrypted with strong cryptography.	- For each sampled system component: i. Describe how administrator access to web-based management interfaces is configured to require strong cryptography. ii. Describe how administrator access to the web-based management interfaces was observed to confirm that all such access is encrypted with strong cryptography.	✓			✓	
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*	**2.4** 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.	- Identify whether the assessed entity is a shared hosting provider. - If the entity is a shared hosting provider, identify here that *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers* has been completed and is included in the ROC.				✓	
Requirement 3: Protect stored cardholder data							
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.	**3.1** Obtain and examine the policies, procedures and processes for data retention and disposal, and perform the following:						
3.1.1 Implement a data retention and disposal policy that includes: - Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements. - Processes for secure deletion of data when no longer needed. - Specific retention requirements for cardholder data. - A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	**3.1.1.a** Verify that policies and procedures are implemented and include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons).	- Identify the documented policies and procedures that: i. Define the legal, regulatory, and business requirements for data retention ii. Specifically address retention requirements for cardholder data - Identify the responsible personnel interviewed who confirm: i. The legal, regulatory, and business requirements that retention requirements are based on ii. That the documented policies and procedures for data retention are implemented		✓	✓		
	3.1.1.b Verify that policies and procedures include provisions for secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data.	- Identify the documented policies and procedures which define processes for secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data. - Briefly describe the implemented processes.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	3.1.1.c Verify that policies and procedures include coverage for all storage of cardholder data.	• Describe how the documented policies and procedures were verified to include coverage for all storage of cardholder data.		✓			
	3.1.1.d Verify that policies and procedures include at least one of the following: ▪ A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy • Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.	• Identify the documented policies and procedures that: i. Define processes for ensuring that stored cardholder data does not exceed requirements defined in the data retention policy ii. Require that the processes be performed at least quarterly • Describe the implemented processes (may be a programmatic process, requirements for a review, or a combination of both).		✓		✓	
	3.1.1.e For a sample of system components that store cardholder data, verify that the data stored does not exceed the requirements defined in the data retention policy.	• Identify the sample of system components that store cardholder data. • For each sampled system component, describe how it was observed that data stored does not exceed the requirements of data retention and disposal policy.				✓	✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: ***Note:*** *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.*	**3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, verify there is a business justification for the storage of sensitive authentication data, and that the data is secured.	• Identify whether the assessed entity is an issuer or supports issuing services. • If the assessed entity is an issuer or supports issuing services: i. Identify and describe the business justification for storing sensitive authentication data. ii. Identify the responsible personnel interviewed who confirm the business justification. iii. Describe how the data was observed to be secured.			✓	✓	
	3.2.b For all other entities, if sensitive authentication data is received and deleted, obtain and review the processes for securely deleting the data to verify that the data is unrecoverable.	• For all instances where sensitive authentication data is received and deleted: i. Identify the document defining the processes for securely deleting sensitive authentication data. ii. Describe how the processes for securely deleting the data were verified to render the data unrecoverable.		✓		✓	
	3.2.c For each item of sensitive authentication data below, perform the following steps:						
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*	**3.2.1** 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 under any circumstance: • 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 observed. • For each sampled system component, identify the observed data sources, including: i. Incoming transaction data ii. All logs (for example, transaction, history, debugging, error) iii. History files iv. Trace files v. Several database schemas vi. Database contents vii. Any other data sources in scope • For each sampled system component and data source, describe how observation of the data sources confirms that full track data is not stored under any circumstance.				✓	✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	**3.2.2** 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 under any circumstance: • 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 observed. • For each sampled system component, identify the observed data sources, including: i. Incoming transaction data ii. All logs (for example, transaction, history, debugging, error) iii. History files iv. Trace files v. Several database schemas vi. Database contents vii. Any other data sources in scope • For each sampled system component and data source, describe how observation of the data sources confirms that card verification codes or values (CVV2, CVC2, CID, CAV2) are not stored under any circumstance.				✓	✓
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**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 under any circumstance: • 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 observed. • For each sampled system component, identify the observed data sources, including: i. Incoming transaction data ii. All logs (for example, transaction, history, debugging, error) iii. History files iv. Trace files v. Several database schemas vi. Database contents vii. Any other data sources in scope • For each sampled system component and data source, describe how observation of the data sources confirms that PINs or encrypted PIN blocks are not stored under any circumstance.				✓	✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). ***Notes:*** • *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.* • *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*	**3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.	• Identify all instances where primary account numbers (PAN) is displayed. • Identify the document that: i. Requires PAN is masked when displayed, except for those with a legitimate business need to see full PAN. ii. Identifies those with a legitimate business need to see full PAN • For all instances where PAN is displayed, describe how PAN was observed to be masked, except where there is a legitimate business need to view the full PAN.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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 should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	**3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). 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 all instances where PAN is stored (including system components, portable digital media, backup media, and in logs). • For each instance of stored PAN: i. Identify the documents describing the methods for protecting the PAN. ii. Briefly describe the implemented methods—including the vendor, type of system/process, and the encryption algorithms (if applicable)—used to protect the PAN. iii. Describe how the implemented methods render the PAN unreadable using any of the following defined 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		✓		✓	
	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 observed. • Identify the tables or files examined within each sampled data repository. • For each table or file examined from each sampled data repository, describe how the observed data confirms PAN is rendered unreadable.				✓	✓
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.	• Identify the sample of removable media observed. • For each item in the sample, describe how PAN was observed to be 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 observed. • For each item in the sample, describe how PAN was observed to be rendered unreadable or removed.				✓	✓

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).	• Identify whether disk encryption is used. • If disk encryption is used: i. Describe the observed disk encryption mechanisms in use. ii. For each disk encryption mechanism in use, describe how the disk encryption mechanism was observed to be separate from the native operating systems mechanism (that is, logical access to the encrypted file system is managed independently of the native operating system access controls)	✓			✓	
	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	• If disk encryption is used, describe how cryptographic keys were observed to be stored securely.				✓	
	3.4.1.c 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.*	• If disk encryption is used, describe how cardholder data on removable media was observed to be encrypted wherever stored.				✓	
3.5 Protect any keys used to secure cardholder data against disclosure and misuse: ***Note:*** *This requirement 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** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:						
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 observed user access lists for cryptographic key storage. • For each key storage location, describe how observed user access lists confirm that access to keys is restricted to the fewest number of custodians necessary.	✓			✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2.a** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.	• Describe how system configuration files were observed to confirm that: i. Keys are stored in encrypted form. ii. Key-encrypting keys are stored separately from data encrypting keys.	✓			✓	
	3.5.2.b Identify key storage locations to verify that keys are stored in the fewest possible locations and forms.	• Identify all locations where keys are stored. • Describe how the observed locations confirm that keys are stored in the fewest possible locations and forms.				✓	
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***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** Verify the existence of key-management procedures for keys used for encryption of cardholder data.	• Identify the documents defining key-management procedures for keys used for encryption of cardholder data.		✓			
	3.6.b For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store, and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	*If the entity being assessed is a service provider:* • Identify whether the service provider shares keys with their customers for transmission or storage of cardholder data. • If keys are shared with customers: i. Identify the document providing customers guidance on how to securely transmit, store, and update customers' keys in accordance with Requirements 3.6.1 through 3.6.8 ii. Describe how the document was observed to be provided to customers.		✓		✓	
	3.6.c Examine the key-management procedures and perform the following:						
3.6.1 Generation of strong cryptographic keys	**3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys.	• Identify the document that defines procedures for the generation of strong keys. • Describe how the procedures for the generation of strong keys were observed to be implemented.		✓		✓	
3.6.2 Secure cryptographic key distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution.	• Identify the document that defines procedures for secure key distribution. • Describe how the procedures for secure key distribution were observed to be implemented.		✓		✓	
3.6.3 Secure cryptographic key storage	**3.6.3** Verify that key-management procedures are implemented to require secure key storage.	• Identify the document that defines procedures for secure key storage. • Describe how the procedures for secure key storage were observed to be implemented.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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** Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.	• Identify the document that defines: i. Key cryptoperiod(s) ii. The procedures for periodic key changes at the end of the defined cryptoperiod(s) • Describe how the procedures for periodic key changes at the end of the defined cryptoperiod(s) were observed to be implemented.		✓		✓	
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. ***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 are implemented to require the retirement of keys when the integrity of the key has been weakened.	• Identify the document that defines procedures for the retirement of keys when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key). • Describe how the procedures for retirement of keys when the integrity of the key has been weakened were observed to be implemented.		✓		✓	
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.	• Identify the document that defines procedures for the replacement of known or suspected compromised keys. • Describe how the procedures for replacement of known or suspected compromised keys were observed to be implemented.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	3.6.5.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.	• Identify whether retired or replaced cryptographic keys are retained. • If retired or replaced cryptographic keys are retained: i. Identify the document which requires that these keys: o Are securely archived o Are not used for encryption operations ii. Describe how the keys were observed to be: o Securely archived o 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 (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). ***Note:*** *Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	**3.6.6** Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.	• Identify whether manual clear-text cryptographic key management operations are used. • If manual clear-text cryptographic key management operations are used: i. Identify the document that defines procedures requiring: o Split knowledge of keys o Dual control of keys ii. Describe how the following procedures were observed to be implemented for manual clear-text cryptographic key operations: o Split knowledge of keys o Dual control of keys		✓		✓	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	**3.6.7** Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.	• Identify the document that defines procedures for prevention of unauthorized substitution of keys. • Describe how the procedures for the prevention of unauthorized substitution of keys were observed to be implemented.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	**3.6.8** Verify that key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	• Identify the document that defines procedures for key custodians to acknowledge that they understand and accept their key-custodian responsibilities. • Describe how key custodian acknowledgements were observed to be implemented. • Identify the key custodians interviewed who confirm that they understand and accept their key-custodian responsibilities.		✓	✓	✓	
Requirement 4: Encrypt transmission of cardholder data across open, public networks							
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:* • The Internet • Wireless technologies, • Global System for Mobile communications (GSM) • General Packet Radio Service (GPRS).	**4.1** Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks. Verify that strong cryptography is used during data transmission, as follows:	• Identify all instances where cardholder data is transmitted or received over open, public networks. • For each identified instance: i. Describe the observed security protocols in use. ii. Describe how configurations were observed to use strong cryptography.	✓			✓	
	4.1.a Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.	• Identify the number and types of transactions sampled. • For each sampled transaction, describe how cardholder data was observed to be encrypted during transit				✓	✓
	4.1.b Verify that only trusted keys and/or certificates are accepted.	• For all instances where cardholder data is transmitted or received over open, public networks: i. Describe the mechanisms used to ensure that only trusted keys and/or certificates are accepted. ii. Describe how the mechanisms were observed to accept only trusted keys and/or certificates.	✓			✓	
	4.1.c 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: i. Describe how the observed protocol configuration and implementation confirms that: ○ The security protocols are implemented to use only secure configurations. ○ The protocol implementation does not support insecure versions or configurations.	✓			✓	
	4.1.d 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: i. Identify vendor recommendations/ best practices for encryption strength. ii. Identify the encryption strength observed to be implemented.		✓		✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	4.1.e For SSL/TLS implementations: - Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). - Verify that no cardholder data is required when HTTPS does not appear in the URL.	- For all instances where SSL/TLS is used to encrypt cardholder data over open, public networks: i. Describe how observed configurations and processes confirm that: o HTTPS appears as a part of the browser URL. o There is no cardholder data required when HTTPS does not appear in the URL.	✓			✓	
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 was prohibited as of 30 June 2010.*	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.	- Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. - For each identified wireless network: i. Identify the industry best practices used to implement: o Strong encryption for authentication o Strong encryption for transmission ii. Describe how observed wireless configurations and processes confirm that industry best practices are implemented for: o Strong encryption for authentication o Strong encryption for transmission	✓	✓		✓	
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	**4.2.a** Verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	- Identify all instances where PAN is sent via end-user messaging technologies. - For each identified instance: i. Describe the method used for securing PAN or rendering it unreadable for each end-user messaging technology used. ii. Describe how the method was observed to be implemented whenever PAN is sent via these technologies.	✓			✓	
	4.2.b Verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.	- Identify the policy document which states that unprotected PANs must not be sent via end-user messaging technologies.		✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 5: Use and regularly update anti-virus software or programs							
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**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 observed (include all operating system types commonly affected by malicious software). • For each sampled system component, describe how anti-virus software was observed to be deployed.	✓				✓
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** For a sample of system components**,** verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).	• Identify the sample of system components observed. • For each sampled system component, describe how anti-virus programs were observed to: i. Detect all known types of malicious software. ii. Remove all known types of malicious software. iii. Protect against all known types of malicious software.	✓				✓
5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	**5.2** Verify that all anti-virus software is current, actively running, and generating logs by performing the following:						
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.	• Identify the policy document that requires updating of anti-virus software and definitions.		✓			
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.	• For each master installation, describe how observed configurations and processes confirm that: i. Anti-virus software is configured for automatic updates. ii. Anti-virus software is configured for periodic scans. iii. Automatic updates are performed. iv. Periodic scans are performed.	✓			✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.	• Identify the sample of system components observed (include all operating system types commonly affected by malicious software). • For each sampled system component, describe how observed configurations and processes confirm that: i. Anti-virus software is configured for automatic updates. ii. Anti-virus software is configured for periodic scans. iii. Automatic updates are performed. iv. Periodic scans are performed.	✓			✓	✓
	5.2.d For a sample of system components, verify that anti-virus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7.	• Identify the sample of system components observed. • For each sampled system component: i. Describe how anti-virus software log generation was observed to be enabled. ii. Describe how anti-virus logs were observed to be retained in accordance with PCI DSS Requirement 10.7, as follows: ○ Audit logs are available for at least one year. ○ Processes are in place to immediately restore at least the last three months' logs for analysis.	✓			✓	✓

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 6: Develop and maintain secure systems and applications							
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. ***Note:*** *An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	**6.1.a** 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 that current vendor patches are installed.	• Identify the sample of system components observed. • Identify the related software observed on each system component. • For each item in the sample: i. Identify the vendor security patch list reviewed. ii. Describe how current vendor security patches for the system component and/or related software were observed to be installed.		✓		✓	✓
	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.	• Identify the document requiring that all critical new security patches are installed within one month.		✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology: Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. ***Notes:*** • *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.* • *The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.*	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities, and that a risk ranking is assigned to such vulnerabilities. (At minimum, the most critical, highest risk vulnerabilities should be ranked as "High.")	• Identify the responsible personnel interviewed who confirm: i. That processes are in place to identify new security vulnerabilities ii. Whether a risk ranking is assigned to such vulnerabilities • If risk ranking *is* assigned to new vulnerabilities, briefly describe the observed process for assigning a risk ranking, including how critical, highest risk vulnerabilities are ranked as "High"[*] *(Note: The ranking of vulnerabilities is considered a best practice until June 30, 2012, after which it becomes a requirement.)*			✓	✓*	
	6.2.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information.	• Identify the document requiring that outside sources are used to identify new security vulnerabilities. • Identify the outside sources used. • Describe how processes were observed to use outside sources to identify new security vulnerabilities.		✓		✓	
6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	**6.3.a** Obtain and 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 practice. • 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 that include information security throughout the software development 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 that specify how software applications are developed in accordance with PCI DSS.		✓			
	6.3.d From an examination of written software development processes, and interviews of software[†] developers, verify that:						

[*] The reporting detail for *"Observe process, action state"* is not required until June 30, 2012.

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	**6.3.1** Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.	• Identify the document requiring removal of custom application accounts, user IDs and/or passwords before the system goes into production or is released to customers. • Identify the responsible personnel interviewed who confirm that custom application accounts, user IDs and/or passwords are removed before the system goes into production or is released to customers.		✓	✓		
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. ***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. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	**6.3.2.a** Obtain and review policies to confirm 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 policy document requiring that all custom application code changes must be reviewed. • Describe the documented processes used for reviewing custom application code changes (for example, manual or automated, or a combination of both). • Identify the documents which define processes for custom application code reviews, and confirm the documented processes require the following: i. All custom application code changes are reviewed. ii. Code changes are reviewed by individuals other than the original author. iii. Code changes are reviewed by individuals who are knowledgeable in code review techniques. iv. Code changes are reviewed by individuals who are knowledgeable in secure coding practices. v. Code reviews ensure secure coding guidelines have been followed. vi. Any corrections identified during the code review are implemented prior to release. vii. Code review results are reviewed by management prior to release. viii. Code review results are approved by management prior to release.		✓			

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	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 custom application changes. • For each sampled application change, describe how the following code review processes were observed to be implemented: i. All custom application code changes are reviewed. ii. Code changes are reviewed by individuals other than the original author. iii. Code changes are reviewed by individuals who are knowledgeable in code review techniques. iv. Code changes are reviewed by individuals who are knowledgeable in secure coding practices. v. Code reviews ensure secure coding guidelines have been followed. vi. Any corrections identified during the code review are implemented prior to release. vii. Code-review results are reviewed by management prior to release. viii. Code review results are 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** From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following:						
6.4.1 Separate development/test and production environments	**6.4.1** The development/test environments are separate from the production environment, with access control in place to enforce the separation.	• Identify the document that defines and/or illustrates: i. How the development/test environment is separated from the production environment. ii. Access controls to enforce separation. • Identify the system and/or network administrators interviewed who confirm: i. The development/test environment is separated from the production environment. ii. Access controls are in place to enforce separation. • Describe how the development/test environment was observed to be separate from the production environment. • Describe the access controls observed to enforce the separation.	✓	✓	✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
6.4.2 Separation of duties between development/test and production environments	**6.4.2** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.	• Identify the document that defines separation of duties between personnel assigned to the development/test environment and those assigned to the production environment. • Briefly describe how separation of duties is implemented. • Identify the personnel assigned to the development/test environments and those assigned to the production environment who were interviewed to confirm that separation of duties is in place. • Describe how separation of duties was observed to be implemented		✓	✓	✓	
6.4.3 Production data (live PANs) are not used for testing or development	**6.4.3** Production data (live PANs) are not used for testing or development.	• Identify the document that defines processes for ensuring: i. Live PANs are not used for testing. ii. Live PANs are not used for development. • Identify the development, test and/or production personnel interviewed who confirm: i. Live PANs are not used for testing. ii. Live PANs are not used for development. • Describe how it was observed that: i. Live PANs are not used for testing. ii. Live PANs are not used for development.		✓	✓	✓	
6.4.4 Removal of test data and accounts before production systems become active	**6.4.4** Test data and accounts are removed before a production system becomes active.	• Identify the document that defines processes for: i. Removing test data before a production system becomes active. ii. Removing test accounts before a production system becomes active. • Identify the development, test and/or production personnel interviewed who confirm: i. Test data are removed before a production system becomes active. ii. Test accounts are removed before a production system becomes active. • Describe the processes observed to be implemented for: i. Removing test data before a production system becomes active. ii. Removing test accounts before a production system becomes active.		✓	✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	**6.4.5.a** Verify that change-control procedures related to implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4 below.	• Identify the document that defines change control procedures for implementation of security patches and software modifications. • Confirm that the documented procedures require the following for all changes: i. Documentation of impact ii. Documented approval by authorized parties iii. Testing of functionality to ensure the change does not adversely impact the security of the system iv. Testing of all custom code updates for compliance with PCI DSS Requirement 6.5 (to address the vulnerabilities identified in 6.5.1 – 6.5.9) v. Back-out procedures		✓			
	6.4.5.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:						
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.	• Identify the sample of: i. System components ii. Recent changes/security patches • For each sampled change, describe how documentation of the impact of the change is included in the change control documentation.		✓			✓
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.	• Identify the sample of: i. System components ii. Recent changes/security patches • For each sampled change, describe how documented approval by authorized parties is included in the change control documentation.		✓			✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology: Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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.	• Identify the sample of: i. System components ii. Recent changes/security patches • For each sampled change: i. Describe how details of functionality testing are included in the change control documentation. ii. Describe how the functionality testing performed verifies 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: i. System components ii. Recent custom code changes/updates • For each sampled custom code change: i. Describe how details of testing for compliance with PCI DSS Requirement 6.5 (to address the vulnerabilities defined in 6.5.1 – 6.5.9) are included in the change control documentation. ii. Describe how the testing performed verifies that all updates are compliant with PCI DSS Requirement 6.5 (6.5.1 – 6.5.9) 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.	• Identify the sample of: i. System components ii. Recent changes/security patches • For each sampled change: i. Describe how details of back-out procedures are included in the change control documentation. ii. Describe how the back-out procedures were observed to be prepared for each change.		✓		✓	✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: ***Note:** The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*	**6.5.a** Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and guidance.	• Identify the document requiring that developers are trained in secure coding techniques. • Identify the industry best practices and guidance that training is based on.		✓			
	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.	• Identify the sample of developers interviewed. • Describe how the interviewed personnel demonstrated they are knowledgeable in secure coding techniques.			✓		✓
	6.5.c. Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:						
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)	• Identify the document that defines the process for ensuring all applications are not vulnerable to injection flaws, particularly SQL injection. • Describe the processes observed to be in place for ensuring that all applications are not vulnerable to injection flaws, particularly SQL injection.		✓		✓	
6.5.2 Buffer overflow	**6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.)	• Identify the document that defines the process for ensuring all applications are not vulnerable to buffer overflow. • Describe the processes observed to be in place for ensuring that all applications are not vulnerable to buffer overflow.		✓		✓	
6.5.3 Insecure cryptographic storage	**6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws)	• Identify the document that defines the process for ensuring all applications are not vulnerable to insecure cryptographic storage. • Describe the processes observed to be in place for ensuring that all applications are not vulnerable to insecure cryptographic storage.		✓		✓	
6.5.4 Insecure communications	**6.54** Insecure communications (Properly encrypt all authenticated and sensitive communications)	• Identify the document that defines the process for ensuring all applications are not vulnerable to insecure communications. • Describe the processes observed to be in place for ensuring that all applications are not vulnerable to insecure communications.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
6.5.5 Improper error handling	**6.5.5** Improper error handling (Do not leak information via error messages)	• Identify the document that defines the process for ensuring all applications are not vulnerable to improper error handling. • Describe the processes observed to be in place for ensuring that all applications are not vulnerable to improper error handling.		✓		✓	
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). ***Note:*** *This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.*	**6.5.6** All "High" vulnerabilities as identified in PCI DSS Requirement 6.2.	• Identify whether a process is in place to ensure all applications are not vulnerable to "High" vulnerabilities as identified in PCI DSS Requirement 6.2. • If there *is* a process in place: i. Identify the document that defines the process for ensuring that all applications are not vulnerable to "High" vulnerabilities as identified in PCI DSS Requirement 6.2. ii. Describe the processes observed to be in place for ensuring that applications are not vulnerable to all "High" vulnerabilities, as identified in PCI DSS Requirement 6.2.		✓		✓	
Note: *Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):*							
6.5.7 Cross-site scripting (XSS)	**6.5.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)	• Identify the document that defines the process for ensuring web applications and application interfaces are not vulnerable to cross-site scripting (XSS). • Describe the processes observed to be in place for ensuring that web applications and application interfaces are not vulnerable to cross-site scripting (XSS).		✓		✓	
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	**6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)	• Identify the document that defines the process for ensuring web applications and application interfaces are not vulnerable to improper access control. • Describe the processes observed to be in place for ensuring that web applications and application interfaces are not vulnerable to improper access control.		✓		✓	
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)	• Identify the document that defines the process for ensuring web applications and application interfaces are not vulnerable to cross-site request forgery. • Describe the processes observed to be in place for ensuring that web applications and application interfaces are not vulnerable to cross-site request forgery.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing a web-application firewall in front of public-facing web applications	**6.6** For *public-facing* web applications, ensure that *either* one of the following methods are in place as follows: • 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 all vulnerabilities are corrected – That the application is re-evaluated after the corrections • Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. ***Note:*** *"An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.*	• For each public-facing web application: i. Identify which of the two methods are implemented (web application vulnerability security assessments, web application firewalls, or both).				✓	
		• If application vulnerability security assessments are performed: i. Describe the tools and/or methods used (manual or automated, or a combination of both). ii. Describe how it was observed that assessments are performed: ○ At least annually ○ After any changes iii. Identify the organization(s) performing the assessments. iv. Identify the responsible personnel interviewed, and describe how those reviewing the applications were confirmed to: ○ Specialize in application security ○ Demonstrate independence from the development team v. Describe the observed process which confirm that: ○ All identified vulnerabilities are corrected. ○ Applications are re-evaluated after the corrections are applied.			✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
		- If a web-application firewall(s) is used: i. Describe how the web-application firewall was observed to be placed in front of all public-facing web applications. ii. Describe the observed web-application firewall configurations for: ○ Detecting web-based attacks ○ Preventing web-based attacks iii. Describe how the web-application firewall was observed to: ○ Detect web-based attacks ○ Prevent web-based attacks	✓			✓	
Requirement 7: Restrict access to cardholder data by business need to know							
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	**7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following:						
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	**7.1.1** Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.	- Identify the data control policy document which requires that access rights for privileged user IDs are restricted to the least privileges necessary to perform job responsibilities.		✓			
7.1.2 Assignment of privileges is based on individual personnel's job classification and function	**7.1.2** Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).	- Identify the data control policy document requiring that privileges are assigned to individuals based on job classification and function.		✓			
7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	**7.1.3** Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges.	- Identify the data control policy document that requires the following: i. Documented approval by authorized parties for all access. ii. That documented approval must specify the required privileges.		✓			
7.1.4 Implementation of an automated access control system	**7.1.4** Confirm that access controls are implemented via an automated access control system.	- Identify the data control policy document requiring that access controls are implemented using an automated access control system.		✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**7.2** 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.	• Describe the access control systems in use. • Describe how access control systems were observed to be 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.	• For each access control system in use: i. Identify the documents that describe: ○ Job classifications and functions ○ The associated privilege assignments ii. Describe how the access control systems were observed to enforce privileges assigned to individuals based on job classification and function.	✓	✓			
7.2.3 Default "deny-all" setting ***Note:*** *Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*	**7.2.3** Confirm that the access control systems have a default "deny-all" setting.	• For each access control system in use: i. Describe how the access control system was observed to have a default "deny-all" setting.	✓				
Requirement 8: Assign a unique ID to each person with computer access							
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data.	• Identify the document requiring that users are assigned a unique ID before being allowed to access system components or cardholder data. • Describe how implemented access control systems were observed to assign unique IDs for access to system components and cardholder data. • Describe how IDs with access to system components or cardholder data were observed be unique.	✓	✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: • Obtain and 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, and confirm 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: i. Describe how the authentication method was observed to be used for access to the cardholder data environment. ii. Describe how the authentication method was observed to be functioning consistent with the documented authentication method(s).		✓		✓	
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) ***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.*	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that two of the three authentication methods are used.	• Identify the document that requires two-factor authentication for remote access by: i. Employees (users) ii. Administrators iii. Third parties • Describe the two-factor authentication technologies implemented for remote access to the network. • For each identified technology: i. Identify the personnel (for example, an administrator) observed connecting remotely to the network. ii. Describe how two-factor authentication was observed to be required for remote access to the network. iii. Identify which two factors are used: ○ Something you know ○ Something you are ○ Something you have		✓		✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	**8.4.a** For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.	• Identify the sample of system components observed. • For each sampled system component, describe how the observed password files verify that passwords are unreadable during: i. Transmission ii. Storage • For each sampled system component, describe how the observed system configuration settings verify that strong cryptography is used for passwords during: i. Transmission ii. Storage	✓			✓	✓
	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.	*If the entity being assessed is a service provider:* • Describe how observed customer password files verify that customer passwords are encrypted during: i. Transmission ii. Storage • Describe how observed system configuration settings confirm that customer passwords are rendered unreadable using strong cryptography during: i. Transmission ii. Storage	✓			✓	
8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	**8.5** Review procedures and interview personnel to verify that procedures are implemented for user identification and authentication management, by performing the following:						

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**8.5.1** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to policy by performing the following: • Obtain and examine an authorization form for each ID. • Verify that the sampled user IDs are implemented in accordance with the authorization form (including all privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.	• Identify the samples of: i. Administrator user IDs ii. General user IDs • For each sampled administrator user ID, describe how the observed authorization forms and system settings confirm that: i. The administrator ID is implemented in accordance with the authorization form. ii. The administrator ID is implemented with the privileges specified on the authorization form. iii. All the appropriate signatures are obtained for authorization. • For each sampled general user ID, describe how the observed authorization forms and system settings confirm that: i. The user ID is implemented in accordance with the authorization form. ii. The user ID is implemented with the privileges specified on the authorization form. iii. All the appropriate signatures are obtained for authorization.	✓	✓			✓
8.5.2 Verify user identity before performing password resets.	**8.5.2** Examine password/authentication procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.	• Describe the non-face-to-face methods used for requesting password resets. • For each non-face-to-face method used: i. Identify the documented procedures for the non-face-to-face method, and confirm the procedures require a user's identity to be verified before the password is reset. ii. Describe how security personnel responsible for resetting passwords were observed to verify user identities before resetting the password.		✓		✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	**8.5.3** 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 procedures for issuing first-time passwords for new users, and confirm the procedures require: i. First-time passwords must be set to a unique value for each user. ii. First-time passwords must be changed after the first use. • Describe how security personnel responsible for assigning first-time passwords were observed to: i. Set first-time passwords to a unique value for each new user. ii. Set first-time passwords to be changed after first use. • Identify the documented procedures for resetting passwords for existing users, and confirm the procedures require: i. Reset passwords must be set to a unique value for each user. ii. Reset passwords must be changed after the first use. • Describe how security personnel responsible for resetting passwords were observed to: i. Set reset passwords to a unique value for each existing user. ii. Set reset passwords to be changed after first use.		✓		✓	
8.5.4 Immediately revoke access for any terminated users.	**8.5.4** Select a sample of users terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.	• Identify the document requiring that access be immediately revoked for any terminated users. • Identify the sample of users terminated in the past six months. • For each sampled user, describe how the user account was observed to be deactivated or removed from user access lists.	✓	✓			✓
8.5.5 Remove/disable inactive user accounts at least every 90 days.	**8.5.5** Verify that inactive accounts over 90 days old are either removed or disabled.	• Identify the document requiring that inactive user accounts over 90 days old are either removed or disabled. • Describe how user accounts inactive for more than 90 days were observed to be disabled or removed.	✓	✓			

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	**8.5.6.a** Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor.	• Identify the document requiring that accounts used by vendors to access, support and maintain system components are: i. Disabled when not being used ii. Enabled only when needed • Briefly describe the implemented processes for: i. Disabling vendor accounts when not being used. ii. Enabling vendor accounts only when needed. • Describe how vendor accounts were observed to be enabled or disabled according to the documented processes.	✓	✓		✓	
	8.5.6.b Verify that vendor remote access accounts are monitored while being used.	• Identify the document requiring that accounts used by vendors are monitored while being used. • Describe how vendor accounts were observed to be monitored while being used.		✓		✓	
8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	**8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with authentication procedures and policies.	• Identify the sample of user IDs. • For each user ID in the sample, describe how the interviewed users demonstrated that they are familiar with authentication procedures and policies.			✓		✓
8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	**8.5.8.a** For a sample of system components, examine user ID lists to verify the following: • Generic user IDs and accounts 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 observed. • For each sampled system component, describe how observed user ID lists verify that: i. Generic user IDs and accounts are disabled or removed. ii. Shared user IDs for system administration activities and other critical functions do not exist. • For each sampled system component, identify personnel with administrator IDs who were interviewed, and who confirm that: i. Shared user IDs are not used to administer any system components. ii. Generic user IDs are not used to administer any system components.	✓		✓		✓
	8.5.8.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.	• Identify the documented policies/procedures which explicitly prohibit: i. Group passwords or other authentication methods ii. Shared passwords or other authentication methods		✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	8.5.8.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.	• Identify the system administrators interviewed who verify that the following are never distributed, even if requested: i. Group passwords or other authentication methods ii. Shared passwords or other authentication methods			✓		
8.5.9 Change user passwords at least every 90 days.	**8.5.9.a** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.	• Identify the sample of system components observed. • For each sampled system component: i. Describe the system configuration settings inspected. ii. Identify how often users are required to change their passwords, as observed in the system configuration settings.	✓				✓
	8.5.9.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to change periodically and that non-consumer users are given guidance as to when, and under what circumstances, passwords must change.	*If the entity being assessed is a service provider:* • Identify the customer/user documentation that provides the following guidance to non-consumer users: i. When to change their passwords ii. Under what circumstances passwords must change • Describe how the documented guidance was observed to be given to non-consumer users. • Describe how the service provider's processes for non-consumer user passwords were observed to include: i. Requirement for non-consumer user passwords to change periodically ii. Details of when non-consumer user passwords must change iii. Details of circumstances that would require a non-consumer user password change		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
8.5.10 Require a minimum password length of at least seven characters.	**8.5.10.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.	• Identify the sample of system components observed. • For each sampled system component: i. Describe the system configuration settings inspected. ii. Identify the required minimum password length observed in the system configuration settings.	✓				✓
	8.5.10.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to meet minimum length requirements.	*If the entity being assessed is a service provider:* • Identify the customer/user documentation that requires non-consumer user passwords to meet minimum length requirements. • Describe how the observed processes confirm that non-consumer user passwords meet minimum password-length requirements.		✓		✓	
8.5.11 Use passwords containing both numeric and alphabetic characters.	**8.5.11.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.	• Identify the sample of system components observed. • For each sampled system component: i. Describe the system configuration settings inspected. ii. Identify the types of characters required for passwords, as observed in the system configuration settings.	✓				✓
	8.5.11.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to contain both numeric and alphabetic characters.	*If the entity being assessed is a service provider:* • Identify the customer/user documentation that requires non-consumer user passwords to use both numeric and alphabetic characters. • Describe how the observed processes confirm that non-consumer user passwords contain both numeric and alphabetic characters.		✓		✓	
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	**8.5.12.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 observed. • For each sampled system component: i. Describe the system configuration settings inspected. ii. Identify the number of previously used passwords that cannot be the same as a new password, as observed in the system configuration settings.	✓				✓

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	8.5.12.b For service providers only, review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords.	*If the entity being assessed is a service provider:* • Identify the customer/user documentation that requires new non-consumer user passwords to not be the same as the previous four passwords. • Describe how the observed processes confirm that new non-consumer user passwords cannot be the same as the previous four passwords.		✓		✓	
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13.a** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.	• Identify the sample of system components observed. • For each sampled system component: i. Describe the system configuration settings inspected. ii. Identify the number of invalid logon attempts that result in user accounts being locked out, as observed in the system configuration settings.	✓				✓
	8.5.13.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user accounts are temporarily locked-out after not more than six invalid access attempts.	*If the entity being assessed is a service provider:* • Identify the customer/user documentation that requires non-consumer user passwords to be temporarily locked out after not more than six invalid access attempts. • Describe how the observed processes confirm that non-consumer user passwords are temporarily locked out after no more than six invalid access attempts.		✓		✓	
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	**8.5.14** For a sample of system components, obtain and 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 observed. • For each sampled system component: i. Describe the system configuration settings inspected. ii. Identify which of the following was observed to be required once a user account is locked out: ○ The user account remains locked for a minimum of 30 minutes; or ○ The user account remains locked until a system administrator resets the account.	✓				✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.5.15** For a sample of system components, obtain and 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 observed. • For each sampled system component: i. Describe the system configuration settings which were inspected. ii. Identify to what time (in minutes) that system and/or session idle time-out features are set, as observed in the system configuration settings. iii. Describe how the system and/or session idle time-out features were observed to require the user to re-authenticate to re-activate the terminal or session.	✓			✓	✓
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	**8.5.16.a** Review database and application configuration settings and verify that all users are authenticated prior to access.	• Identify all databases containing cardholder data. • For each database containing cardholder data: i. Describe how authentication is managed (for example, via application and/or database interfaces). ii. Describe how database and/or application configuration settings were observed to authenticate all users prior to access.	✓			✓	
	8.5.16.b Verify that database and application configuration settings ensure that all 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 containing cardholder data: i. Describe how the observed database and application configuration settings ensure 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 (for example, move, copy, delete) ii. Describe how it was observed 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 (for example, move, copy, delete)	✓			✓	
	8.5.16.c Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators.	• For each database containing cardholder data, describe how database and application configuration settings were observed to restrict the following to only database administrators: i. User direct access to the database ii. User direct queries to the database	✓				

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	8.5.16.d Review database applications 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 containing cardholder data: i. Identify applications with access to the database. ii. Describe the implemented methods for ensuring that application IDs can only be used by the applications, and not by: ○ Individual users ○ Other processes iii. Describe how the methods were observed to ensure that application IDs cannot be used by: ○ Individual users ○ Other processes	✓			✓	
Requirement 9: Restrict physical access to cardholder data							
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**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 computer rooms, data centers and other physical areas with systems in the cardholder data environment. • For each area identified: i. Describe the physical security controls observed. ii. Describe how access was observed to be controlled with badge readers or other devices, including authorized badges and lock and key. iii. Identify the number of randomly selected systems in the cardholder environment for which a system administrator login attempt was observed. iv. Describe how consoles for the randomly selected systems were observed to be "locked".				✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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 the 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.	• Identify and briefly describe all sensitive areas. • For each identified sensitive area: i. Describe the video cameras and/or access control mechanisms observed to monitor the entry/exit points. ii. Describe how the video cameras and/or access control mechanisms were observed to monitor individual physical access to the sensitive area.				✓	
	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: i. Tampering ii. Disabling				✓	
	9.1.1.c Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.	• Describe how the video cameras and/or access control mechanisms were observed to be monitored. • Describe how data from cameras and/or other mechanisms was observed to be reviewed and correlated with other entries. • Describe how data from the cameras and/or access control mechanisms was observed to be stored for at least three months.				✓	
9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized onsite personnel. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.	• Identify the network administrators interviewed who confirm that either: i. Publicly accessible network jacks are enabled only when needed by authorized onsite personnel; or ii. Visitors are escorted at all times in areas with active network jacks. • Describe how it was observed that either: i. Publicly accessible network jacks are enabled only when needed by authorized onsite personnel; or ii. Visitors are escorted at all times in areas with active network jacks.			✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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: i. Wireless access points ii. Wireless gateways iii. Wireless handheld devices iv. Network/communications hardware v. Telecommunication lines				✓	
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	**9.2.a** Review processes and procedures for assigning badges to onsite personnel and visitors, and verify these processes include the following: • Granting new badges, • Changing access requirements, and • Revoking terminated onsite personnel and expired visitor badges	• Identify the documented processes and procedures for assigning badges to onsite personnel, and verify the processes include: i. Granting new badges ii. Changing access requirements iii. Revoking badges for terminated onsite personnel • Describe how the documented procedures for assigning badges to onsite personnel were observed to be implemented, including: i. Granting new badges ii. Changing access requirements iii. Revoking badges for terminated onsite personnel • Identify the documented processes and procedures for assigning badges to visitors, and verify the processes include: i. Granting new badges ii. Changing access requirements iii. Expiration of visitor badges • Describe how the documented procedures for assigning badges to visitors were observed to be implemented, including: i. Granting new badges ii. Changing access requirements iii. Expiration of visitor badges		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	9.2.b Verify that access to the badge system is limited to authorized personnel.	• Identify the document which identifies personnel who are authorized to access the badge system. • Describe how access to the badge system was observed to be restricted to authorized personnel.		✓		✓	
	9.2.c Examine badges in use to verify that they clearly identify visitors and it is easy to distinguish between onsite personnel and visitors.	• Briefly describe the badges observed for onsite personnel and visitors. • Describe how badges clearly identify visitors. • Describe how badges distinguish onsite personnel from visitors.				✓	
9.3 Make sure all visitors are handled as follows:	**9.3** Verify that visitor controls are in place as follows:						
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	**9.3.1** Observe the use of visitor ID badges to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.	• Describe how the use of visitor badges was observed to verify that the visitor ID badge does not permit unescorted access to physical areas that store cardholder data.				✓	
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	**9.3.2.a** Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel.	• Describe how people within the facility were observed to use visitor ID badges. • Describe how observed visitors within the facility are easily distinguished from onsite personnel.				✓	
	9.3.2.b Verify that visitor badges expire.	• Describe how visitor badges were observed to expire.				✓	
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.	• Describe how observed visitors were asked to surrender their ID badge upon departure or expiration.				✓	
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.	• Describe how a visitor log was observed to be in use to record physical access to: i. The facility ii. Computer rooms and data centers where cardholder data is stored or transmitted				✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is retained for at least three months.	• Describe how the visitor log was observed to contain: i. Visitor name ii. Firm represented iii. Onsite personnel authorizing physical access • Identify the defined retention period for visitor logs. • Describe how visitor logs were observed to be retained for at least three months.		✓		✓	
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	**9.5.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 the observed physical security of each storage area ensures that backup media is stored securely.				✓	
	9.5.b Verify that the storage location security is reviewed at least annually.	• Identify the document that defines the process for reviewing the security of each storage location at least annually. • Describe how it was observed that reviews of the security of each storage location are performed at least annually.		✓		✓	
9.6 Physically secure all media.	**9.6** 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, and confirm that the procedures include controls for physically securing all media. • For each type of media used: i. Briefly describe the controls for physically securing the media. ii. Describe how the documented controls were observed to be implemented		✓		✓	
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**9.7** 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 policy document that defines controls for distribution of media. • Describe how the policy covers all distributed media. • Describe how the policy covers media distributed to individuals.		✓			
9.7.1 Classify media so the sensitivity of the data can be determined.	**9.7.1** Verify that all media is classified so the sensitivity of the data can be determined.	• Identify the document that defines how media is classified. • Briefly describe how media is classified to determine sensitivity of the data. • Describe how the classifications were observed to be implemented so the sensitivity of the data can be determined.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.	• Describe how it was observed that all media sent outside the facility is: i. Logged ii. Authorized by management iii. Sent via secured courier or other delivery method that can be accurately tracked.				✓	
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite tracking logs for all media, and verify the presence in the logs of tracking details and proper management authorization.	• Identify the sample of offsite tracking logs for all media. • For each item in the sample, describe how the logs were observed to include: i. Tracking details ii. Proper management authorization				✓	✓
9.9 Maintain strict control over the storage and accessibility of media.	**9.9** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.	• Identify the policy document that defines requirements for: i. Controlling storage of all media ii. Controlling maintenance of all media iii. Periodic inventories for all media • Describe how the policy requirements were observed to be implemented for: i. Controlling storage of all media ii. Controlling maintenance of all media iii. Performing periodic inventories for all media		✓		✓	
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**9.9.1** Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.	• Identify the document that describes the process for conducting media inventories at least annually. • Describe how media inventory logs of all media were observed to be maintained. • Describe how it was observed that media inventories are performed at least annually.		✓		✓	
9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	**9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media, and confirm the following:	• Identify the policy document that defines media destruction requirements. • Confirm that the policy covers all media.		✓			
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	**9.10.1.a** Verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.	• Describe the documented process for destruction of hardcopy materials. • Describe how the observed process provides reasonable assurance that hardcopy materials cannot be reconstructed.		✓		✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access to its contents.	• Describe how the containers used for storing information to be destroyed were observed to be secured.				✓	
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**9.10.2** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).	• Describe the documented process for destruction of electronic media, including details of methods used for: i. Secure wiping of media, and/or ii. Physical destruction of media • Describe how the observed processes ensure that data is rendered unrecoverable. • If data is rendered unrecoverable via secure deletion or a secure wipe program, identify the industry-accepted standards used.		✓		✓	
Requirement 10: Track and monitor all access to network resources and cardholder data							
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.	• Identify the system administrator(s) interviewed who confirm that audit trails are enabled and active for system components. • Describe how audit trails were observed to be enabled and active.			✓	✓	
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:						
10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.	• Identify the responsible personnel interviewed who confirm that all individual access to cardholder data is logged. • Describe how configuration settings were observed to log all individual access to cardholder data. • Describe how observed audit logs include all individual access to cardholder data.	✓		✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify actions taken by any individual with root or administrative privileges are logged.	• Identify the responsible personnel interviewed who confirm that actions taken by any individual with root or administrative privileges are logged. • Describe how configuration settings were observed to log all actions taken by any individual with root or administrative privileges. • Describe how observed audit logs include all actions taken by any individual with root or administrative privileges.	✓		✓	✓	
10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.	• Identify the responsible personnel interviewed who confirm that access to all audit trails is logged. • Describe how configuration settings were observed to log access to all audit trails. • Describe how observed audit logs include access to all audit trails.	✓		✓	✓	
10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.	• Identify the responsible personnel interviewed who confirm that invalid logical access attempts are logged. • Describe how configuration settings were observed to log invalid logical access attempts. • Describe how observed audit logs include invalid logical access attempts.	✓		✓	✓	
10.2 5 Use of identification and authentication mechanisms	**10.2.5** Verify use of identification and authentication mechanisms is logged.	• Identify the responsible personnel interviewed who confirm that the use of identification and authentication mechanisms is logged. • Describe how configuration settings were observed to log the use of identification and authentication mechanisms. • Describe how observed audit logs include use of identification and authentication mechanisms.	✓		✓	✓	
10.2.6 Initialization of the audit logs	**10.2.6** Verify initialization of audit logs is logged.	• Identify the responsible personnel interviewed who confirm that the initialization of audit logs is logged. • Describe how configuration settings were observed to log the initialization of audit logs. • Describe how observed audit logs include initialization of audit logs.	✓		✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.	• Identify the responsible personnel interviewed who confirm that the following are logged: i. Creation of system level objects ii. Deletion of system level objects • Describe how configuration settings were observed to log: i. Creation of system level objects ii. Deletion of system level objects • Describe how observed audit logs include: i. Creation of system level objects ii. Deletion of system level objects	✓		✓	✓	
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation, for each auditable event (from 10.2), perform the following:						
10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.	• For *each auditable event* from 10.2.1 – 10.2.7: i. Identify the responsible personnel interviewed who confirm that user identification is included in log entries. ii. Describe how audit logs were observed to include user identification.			✓	✓	
10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.	• For *each auditable event* from 10.2.1 – 10.2.7: i. Identify the responsible personnel interviewed who confirm that the type of event is included in log entries. ii. Describe how audit logs were observed to include the type of event.			✓	✓	
10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.	• For *each auditable event* from 10.2.1 – 10.2.7: i. Identify the responsible personnel interviewed who confirm that the date and time is included in log entries. ii. Describe how audit logs were observed to include the date and time.			✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.	• For *each auditable event* from 10.2.1 – 10.2.7: i. Identify the responsible personnel interviewed who confirm that success or failure indication is included in log entries. ii. Describe how audit logs were observed to include success or failure indication.			✓	✓	
10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.	• For *each auditable event* from10.2.1 – 10.2.7: i. Identify the responsible personnel interviewed who confirm that origination of the event is included in log entries. ii. Describe how audit logs were observed to include the origination of the event.			✓	✓	
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 *each auditable event* from10.2.1 – 10.2.7: i. Identify the responsible personnel interviewed who confirm that the identity or name of affected data, system component, or resource is included in log entries. ii. Describe how audit logs were observed to include the identity or name of affected data, system component, or resource.			✓	✓	
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	**10.4.a** 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. • Identify the document that defines processes for ensuring the time synchronization technologies are kept current per PCI DSS Requirements 6.1 and 6.2. • Describe how time synchronization technologies were observed to be: i. Implemented ii. Kept current per the documented process	✓	✓		✓	
	10.4.b Obtain and review the process for acquiring, distributing and storing the correct time within the organization, and review the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:						

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.	• Identify the document that defines processes for acquiring, distributing, and storing the correct time within the organization, and confirm the processes require that: i. Only designated central time servers receive time signals from external sources. ii. Time signals from external sources are based on International Atomic Time or UTC. • Identify the sample of system components observed. • Describe how configuration settings observed on the sampled system components confirm that: i. Only designated central time servers receive time signals from external sources. ii. Time signals from external sources are based on International Atomic Time or UTC. • Describe how time synchronization processes were observed to verify: i. Only designated central time servers receive time signals from external sources. ii. Time signals from external sources are based on International Atomic Time or UTC.	✓	✓		✓	✓
	10.4.1.b Verify that the designated central time servers peer with each other to keep accurate time, and that other internal servers receive time only from the central time servers.	• Identify the document requiring that: i. The designated central time servers peer with each other to keep accurate time. ii. Other internal servers receive time only from the central time servers. • Identify the sample of system components observed. • Describe how configuration settings observed on the sampled system components confirm that: i. The designated central time servers peer with each other to keep accurate time. ii. Other internal servers receive time only from the central time servers. • Describe how time synchronization processes were observed to verify: i. The designated central time servers peer with each other to keep accurate time. ii. Other internal servers receive time only from the central time servers.	✓	✓		✓	✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.4.2 Time data is protected.	**10.4.2.a** Review 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 document that: i. Requires that access to time data is restricted to only personnel with a business need to access time data. ii. Defines 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. • Identify the sample of system components observed. • Describe how configuration settings on the sampled system components were observed to restrict access to time data to only personnel with a documented business need.	✓	✓	✓		✓
	10.4.2.b Review system configurations and time synchronization settings and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	• Identify the document that requires: i. Changes to time settings on critical systems are logged ii. Changes to time settings on critical systems are monitored iii. Changes to time settings on critical systems are reviewed • Identify the sample of system components observed. • Describe how configuration settings on the sampled system components were observed to log any changes to time settings on critical systems. • Describe how time synchronization processes were observed to verify: i. Changes to time settings on critical systems are logged ii. Changes to time settings on critical systems are monitored iii. Changes to time settings on critical systems are reviewed	✓	✓		✓	✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.4.3 Time settings are received from industry-accepted time sources.	**10.4.3** Verify that the time servers 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 that defines how time settings are received from industry-accepted time sources. • Describe how configuration settings on time servers were observed to receive time updates from specific, industry-accepted external sources. • Describe how time synchronization processes were observed to verify that the time servers receive time updates from specific, industry-accepted external sources. *Optionally:* • Identify the document that defines how time updates are encrypted with a symmetric key, and access control lists specify the IP addresses of client machines to be provided with the time updates. • Describe how configuration settings on time servers were observed to encrypt time updates with a symmetric key. • Describe how access control lists were observed to specify the IP addresses of client machines to be provided with the time updates. • Describe how time synchronization processes were observed to verify that time updates are encrypted with a symmetric key, and access control lists are implemented to specify the IP addresses of client machines.	✓	✓		✓	
10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:						
10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files.	• Identify the document defining which personnel have a job-related need to view audit trail files. • Identify the authorized personnel interviewed who confirm that all personnel with access to view audit trail files have a business need to do so. • Describe how observed system and audit log permission settings restrict viewing of audit trail files to only individuals who have a documented job-related need. • Describe how observed access to audit logs confirms that only individuals with a job-related need can view the audit trail files.	✓	✓	✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	• Describe the methods used to protect audit trail files from unauthorized modifications (e.g., via access control mechanisms, physical segregation, and/or network segregation). • Describe how system configurations and audit log settings were observed to protect audit trail files from unauthorized modifications. • Describe how observed access to audit logs confirms that audit trail files are protected from unauthorized modifications.	✓			✓	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** 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: i. The centralized log server or media that audit trail files are backed up to ii. How frequently the audit trail files are backed up, and how the frequency Is appropriate iii. How the centralized log server or media is difficult to alter • Identify the responsible personnel interviewed who confirm: i. That current audit trail files are promptly backed up to the centralized log server or media. ii. The frequency that audit trail files are backed up iii. That the centralized log server or media is difficult to alter. • Describe how observed system and audit log settings are configured to promptly back up audit trail files to the centralized log server or media. • Describe how audit logs were observed to be promptly backed up to the centralized log server or media.	✓		✓	✓	
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	**10.5.4** Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.	• Describe how logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media. • Identify the responsible personnel interviewed who confirm that logs for external-facing technologies are offloaded or copied onto a secure, centralized internal log server or media. • Describe how observed external-facing system and audit log settings are configured to offload or copy logs onto a secure centralized internal log server or media. • Describe how logs for external-facing technologies were observed to be located on the centralized internal log server or media.	✓		✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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** Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.	• Identify the file-integrity monitoring (FIM) or change-detection software in use. • Identify the personnel responsible for monitoring FIM and/or change detection software, who were interviewed to confirm that audit log files are monitored. • Describe how system settings were observed to monitor logs to ensure that existing log data cannot be changed without generating alerts. • Describe how observed results from monitoring activities confirm that log data cannot be changed without generating alerts.	✓		✓	✓	
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6*.	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.	• Identify the security policy document which requires: i. Review of logs for all system components, including those that perform security functions, at least daily ii. Follow-up to exceptions • Identify the documented procedures for: i. Reviewing logs for all system components at least daily ii. Following up exceptions • Describe the implemented procedures for: i. Reviewing logs for all system components at least daily ii. Following up exceptions		✓		✓	
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.	• Identify the responsible personnel interviewed who confirm that: i. Log reviews are performed for all system components at least daily ii. Log reviews include follow-up to exceptions • Describe how observed evidence from log reviews confirms that: i. Log reviews are performed for all system components ii. Log reviews include follow-up to exceptions			✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.	• Identify the security policy document that: i. Defines audit log retention policies ii. Requires audit log retention for at least one year. • Identify the document which defines procedures for audit log retention. • Describe how the implemented procedures ensure audit log retention for at least one year.		✓		✓	
	10.7.b Verify that audit logs are available for at least one year and processes are in place to immediately restore at least the last three months' logs for analysis.	• Identify the document that defines the process to immediate restore at least the last three months' logs for analysis. • Describe the implemented processes. • Describe how audit logs and restore processes were observed to confirm that: i. Audit logs are available for at least one year. ii. At least the last three months' logs can be immediately restored for analysis.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 11: Regularly test security systems and processes.							
11.1 Test for the presence of wireless access points and detect 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 any unauthorized devices.*	**11.1.a** Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.	• Identify the document that defines the methods and processes to: i. Detect wireless access points. ii. Identify unauthorized wireless access points. iii. Perform the process (at least) 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 wireless devices connected to system components (for example, by USB, etc.) • Wireless devices attached to a network port or network device	• Describe the documented methodology for detection and identification of unauthorized wireless access points, including: i. WLAN cards inserted into system components ii. Portable wireless devices connected to system components iii. Wireless devices attached to a network port or network device iv. Any other unauthorized wireless access points • Describe how the methodology/processes were observed to be adequate to detect and identify unauthorized wireless access points, including: i. WLAN cards inserted into system components ii. Portable wireless devices connected to system components iii. Wireless devices attached to a network port or network device iv. Any other unauthorized wireless access points		✓		✓	
	11.1.c Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities.	• Identify the personnel who perform the process who were interviewed to confirm that: i. The process is performed at least quarterly ii. The process covers all system components iii. The process covers all facilities • Describe how observed results of previously performed processes confirm that: i. The process is performed at least quarterly ii. The process covers all system components iii. The process covers all facilities			✓	✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.	• Identify and describe any automated monitoring technologies in use (for example, wireless IDS/IPS, NAC, etc.) • For each automated monitoring technology in use: i. Describe how the observed technology is configured to generate alerts to personnel. ii. Describe how alerts to personnel were observed to be generated. iii. Identify the personnel responsible for receiving the alerts, who were interviewed to confirm that the generated alerts are received as intended.	✓		✓	✓	
	11.1.e Verify the organization's incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.	• Identify the Incident Response Plan document that defines response procedures in the event unauthorized wireless devices are detected. • Identify the responsible personnel interviewed who confirm that, in the event unauthorized wireless devices are detected, the documented response is followed.		✓	✓		
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:** It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance 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. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*	**11.2** Verify that internal and external vulnerability scans are performed as follows:						

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
11.2.1 Perform quarterly internal vulnerability scans.	**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 scan report documents that verify four quarterly internal scans occurred in the most recent 12-month period. • For each of the four internal quarterly scans performed in the most recent 12-month period, identify the following: i. Date quarterly scan was performed ii. Result of scan		✓			
	11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all “High” vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.	• Identify the document that defines the process for performing rescans as part of the quarterly internal scan process. • Identify personnel interviewed who confirm that the documented rescan process is followed for quarterly internal scans. • For each of the four internal quarterly scans identified in 11.2.1.a, identify the following: i. Whether a rescan was required ii. Details of how rescans were performed until either: ○ Passing results are obtained, or ○ All “High” vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.		✓	✓		
	11.2.1.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).	• From the scan reports, identify whether internal and/or external resources perform internal quarterly scans. • Identify the interviewed personnel who perform the scans, and describe how the personnel demonstrated they are qualified to perform the scans. • Describe how organizational independence of the tester was observed to exist.		✓	✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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). ***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). Scans conducted after network changes may be performed by internal staff.*	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.	• Identify the external scan report documents that verify four quarterly external scans occurred in the most recent 12-month period.		✓			
	11.2.2.b Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).	• Describe how the external scan reports verify that the scans satisfy the *ASV Program Guide* requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).		✓			
	11.2.2.c Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC.	• Describe how the external scan reports verify that the scans were completed by a PCI SSC-Approved Scanning Vendor (ASV).		✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
11.2.3 Perform internal and external scans after any significant change. ***Note:*** *Scans conducted after changes may be performed by internal staff.*	**11.2.3.a** Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.	• Identify the document that defines the process for performing internal and external scans after any significant change. • Identify whether any significant changes were made to internal and/or external system components during the past 12 months. • Identify change control documentation containing details of the identified changes. • Describe how the change control documentation and scan reports confirm 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 greater than a 4.0 by the CVSS, • For internal scans, a passing result is obtained or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.	• For all scans reviewed in 11.2.3.a, identify the following: i. Whether a rescan was required ii. Details of how rescans were performed until: ○ For external scans – No vulnerabilities with a CVSS score greater than 4.0 exist. ○ For internal scans – Either passing results were obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 were resolved. • Identify personnel interviewed to confirm that the process for performing scans after significant changes includes rescans as defined.		✓	✓		
	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).	• From the scan reports, identify whether internal and/or external resources perform the scans. • Identify the interviewed personnel who perform the scans, and describe how the personnel demonstrated they are qualified to perform the scans. • Describe how organizational independence of the tester was observed to exist.		✓	✓	✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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: i. Internal penetration tests are performed annually. ii. 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: i. Significant internal infrastructure or application upgrade. ii. Significant external infrastructure or application upgrade.		✓		✓	
	11.3.b Verify that noted exploitable vulnerabilities were corrected and testing repeated.	• Identify whether any exploitable vulnerabilities were noted in the most recent: i. Internal penetration test results ii. 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: i. Testing was repeated. ii. All noted exploitable vulnerabilities were corrected.		✓	✓		
	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.			✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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: i. Internal penetration testing includes network-layer penetration tests. ii. External penetration testing includes network-layer penetration tests. iii. The network-layer penetration tests include: o Components that support network functions o Operating systems • Identify the responsible personnel interviewed who confirm that: i. Internal penetration testing includes network-layer penetration tests. ii. External penetration testing includes network-layer penetration tests. iii. The network-layer penetration tests include: o Components that support network functions o Operating systems		✓	✓		
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: i. Internal penetration testing includes application-layer penetration tests. ii. External penetration testing includes application-layer penetration tests. iii. 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: i. Internal penetration testing includes application-layer penetration tests. ii. External penetration testing includes application-layer penetration tests. iii. The application-layer tests include, at a minimum, the vulnerabilities listed in PCI DSS Requirement 6.5.		✓	✓		

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.	• Describe the intrusion-detection and/or intrusion-prevention systems (IDS/IPS) that are implemented. • Describe how IDS/IPS were observed to be positioned within the environment to ensure that all traffic is monitored: i. At the perimeter of the cardholder data environment ii. At critical points within the cardholder data environment • Describe how observed IDS/IPS configurations confirm that all traffic is monitored: i. At the perimeter of the cardholder data environment ii. At critical points within the cardholder data environment	✓			✓	
	11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.	• Describe how observed IDS/IPS are configured to alert personnel of suspected compromises. • Describe how alerts to personnel were observed to be generated. • Identify the personnel responsible for receiving the alerts, who were interviewed to confirm that the generated alerts are received as intended.	✓		✓	✓	
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.	• Identify the document that defines vendor instructions for: i. Configuring IDS/IPS devices ii. Maintaining IDS/IPS devices iii. Updating IDS/IPS devices • Describe how observed IDS/IPS settings and configurations confirm that vendor instructions are followed for: i. Configuring IDS/IPS devices ii. Maintaining IDS/IPS devices iii. Updating IDS/IPS devices	✓	✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For file-integrity monitoring 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. 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 file-integrity monitoring tools 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	• Describe the file-integrity monitoring (FIM) tools deployed. • Describe how FIM settings and configurations were observed to monitor changes to: i. Critical system files ii. Critical configuration files iii. Critical content files • Describe how observed results from monitoring activities confirm that changes to the following files are monitored: i. Critical system files ii. Critical configuration files iii. Critical content files	✓			✓	
	11.5.b Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.	• Describe how observed FIM settings are configured to: i. Alert personnel to unauthorized modification of critical files. ii. Perform critical file comparisons at least weekly. • Describe how results and alerts from monitoring activities were observed to confirm that: i. Personnel are alerted to unauthorized modification of critical files. ii. Critical file comparisons are performed at least weekly. • Identify the responsible personnel who were interviewed to confirm that: i. The generated alerts are received as intended. ii. Critical file comparisons are performed at least weekly.	✓		✓	✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 12: Maintain a policy that addresses information security for all personnel.							
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**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. • Describe how the documented policy was observed to be published and disseminated to: i. All relevant personnel ii. All relevant vendors and business partners • Identify the relevant personnel who were interviewed to confirm that they received the policy.		✓	✓	✓	
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.	• Describe how the policy addresses all applicable PCI DSS requirements.		✓			
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	**12.1.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.	• Identify the document that defines the annual risk assessment process. • Describe how the documented process: i. Identifies threats and vulnerabilities ii. Results in formal risk assessment		✓			
	12.1.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually.	• Describe how observed risk assessment results confirm that: i. The risk assessment process is performed at least annually. ii. The documented risk assessment process was followed.		✓			
12.1.3 Includes a review at least annually and updates when the environment changes.	**12.1.3** 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 requiring that the information security policy is: i. Reviewed at least annually ii. Updated as needed to reflect changes to business objectives or the risk environment • Identify the personnel interviewed who confirm that the information security policy is: i. Reviewed at least annually ii. Updated as needed to reflect changes to business objectives or the risk environment • Describe how it was observed that the information security policy is: i. Reviewed at least annually ii. Updated as needed to reflect changes to business objectives or the risk environment		✓	✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**12.2** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.	• Identify the documented daily operational security procedures. • Describe how the documented procedures: i. Are consistent with PCI DSS requirements ii. Include administrative procedures for each requirement iii. Include technical procedures for each requirement • Describe how the daily operational security procedures were observed to be implemented including: i. Administrative procedures for each requirement ii. Technical procedures for each requirement		✓		✓	
12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	**12.3** Obtain and examine the usage policies for critical technologies and perform the following:						
12.3.1 Explicit approval by authorized parties	**12.3.1** Verify that the usage policies require explicit approval from authorized parties to use the technologies.	• Identify critical technologies in use. • For each identified critical technology: i. Identify the documented usage policies defining proper use of the technology. ii. Describe how the documented policies require explicit approval from authorized parties to use the technology. iii. Describe how explicit approval for use of the technology was observed to be implemented.		✓		✓	
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).	• For each identified critical technology: i. Describe how the documented policies require that use of the technology be authenticated with user ID and password or other authentication item. ii. Describe how the required authentication for use of the technology was observed to be implemented.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices.	• For each identified critical technology: i. Describe how the documented policies require: ○ A list of all devices ○ A list of personnel authorized to use the devices ii. Describe how the following was observed to be implemented: ○ A list of all devices ○ A list of personnel authorized to use the devices		✓		✓	
12.3.4 Labeling of devices to determine owner, contact information and purpose	**12.3.4** Verify that the usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose.	• For each identified critical technology: i. Describe how the documented policies require labeling of devices with information that can be correlated to: ○ Owner ○ Contact information ○ Purpose ii. Describe how labeling was observed to be implemented which correlates to: ○ Owner ○ Contact information ○ Purpose		✓		✓	
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies require acceptable uses for the technology.	• For each identified critical technology: i. Describe how the documented policies require acceptable uses for the technology. ii. Describe how requirements for acceptable uses of the technology were observed to be implemented.		✓		✓	
12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies require acceptable network locations for the technology.	• For each identified critical technology: i. Describe how the documented policies require acceptable network locations for the technology. ii. Describe how requirements for acceptable network locations were observed to be implemented.		✓		✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company-approved products.	• For each identified critical technology: i. Describe how the documented policies require a list of company-approved products. ii. Describe how the list of company-approved products was observed to be implemented.		✓		✓	
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**12.3.8** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	• Identify the remote-access technologies used. • For each remote-access technology: i. Describe how the documented policies require automatic disconnect of sessions after a specific period of inactivity. ii. Describe how automatic disconnect after a specific period of inactivity was observed to be implemented.		✓		✓	
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.	• Identify the remote-access technologies used by vendors and business partners. • For each remote-access technology: i. Describe how the documented policies require: ○ Activation of the technology only when needed ○ Immediate deactivation of the technology after use i. Describe how it was observed that: ○ The technology is activated only when needed. ○ The technology is immediately deactivated after use.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	**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.	• Describe how the documented policies prohibit the following for personnel accessing cardholder data via remote-access technologies: i. Copying of cardholder data onto local hard drives and removable electronic media ii. Moving of cardholder data onto local hard drives and removable electronic media iii. Storage of cardholder data onto local hard drives and removable electronic media • Describe how it was observed that the following are implemented for personnel accessing cardholder data via remote-access technologies: i. Prohibit the copying of cardholder data onto local hard drives and removable electronic media ii. Prohibit the moving of cardholder data onto local hard drives and removable electronic media iii. Prohibit the storage of cardholder data onto local hard drives and removable electronic media		✓		✓	
	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.	• Identify the documentation that defines whether any authorized business need for copying, moving, or storing cardholder data onto local hard drives or removable electronic media via remote-access technologies exists. • For each defined business need: i. Identify how explicit authorization was observed to be implemented for the copying, moving, or storage of cardholder data onto local hard drives or removable electronic media. ii. Describe how the documented policies require the protection of cardholder data in accordance with PCI DSS Requirements, for all personnel with proper authorization. iii. Describe how the protection of cardholder data was observed to be implemented 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** Verify that information security policies clearly define information security responsibilities for all personnel.	• Describe how the security policy and procedures clearly define information security responsibilities for all personnel. • Describe how interviewed personnel demonstrated they are aware of their information security responsibilities.		✓	✓		

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:	• Identify the document that formally assigns responsibility for information security to a Chief Security Officer or other security-knowledgeable member of management. • Describe how the assignment of responsibility for information security was observed to be implemented.		✓		✓	
12.5.1 Establish, document, and distribute security policies and procedures.	**12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned.	• Identify the document that formally assigns responsibility for: i. Creating security policies and procedures ii. Distributing security policies and procedures • Describe how assigned responsibilities were observed to be implemented for: i. Creating security policies and procedures ii. 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.	• Identify the document that formally assigns responsibility for: i. Monitoring and analyzing security alerts ii. Distributing information to appropriate information security and business unit management personnel • Describe how assigned responsibilities were observed to be implemented for: i. Monitoring and analyzing security alerts ii. 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 creating and distributing security incident response and escalation procedures is formally assigned.	• Identify the document that formally assigns responsibility for: i. Creating security incident response and escalation procedures ii. Distributing security incident response and escalation procedures • Describe how assigned responsibilities were observed to be implemented for: i. Creating security incident response and escalation procedures ii. Distributing security incident response and escalation procedures		✓		✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.5.4 Administer user accounts, including additions, deletions, and modifications	**12.5.4** Verify that responsibility for administering user account and authentication management is formally assigned.	• Identify the document that formally assigns responsibility for administering user account and authentication management. • Describe how the assignment of responsibility for administering user account and authentication management was observed to be implemented.		✓		✓	
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.	• Identify the document which formally assigns responsibility for: i. Monitoring all access to data ii. Controlling all access to data • Describe how the assignment of responsibilities were observed to be implemented for: i. Monitoring all access to data ii. 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** Verify the existence of a formal security awareness program for all personnel.	• Identify the document that defines a formal security awareness program for all personnel. • Describe how a formal security awareness program was observed to be implemented for all personnel.		✓		✓	
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:						
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).	• Identify the document defining the methods of communicating awareness and educating personnel. • Identify the methods observed for communicating awareness and educating personnel.		✓		✓	
	12.6.1.b Verify that personnel attend awareness training upon hire and at least annually.	• Identify the document requiring that all personnel attend awareness training: i. Upon hire ii. At least annually • Describe how it was observed that all personnel attend awareness training: i. Upon hire ii. At least annually		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
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.	• Identify the document that requires: i. All personnel to acknowledge that they have read and understand the information security policy. ii. All personnel to provide an acknowledgement at least annually. • Describe how it was observed that: i. All personnel acknowledge that they have read and understand the information security policy. ii. All personnel 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) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment.	• Identify the document requiring that background checks be conducted: i. On potential personnel who will have access to cardholder data or the cardholder data environment ii. Prior to hiring the personnel • Identify the Human Resource personnel who were interviewed to confirm that background checks are conducted: i. On potential personnel who will have access to cardholder data or the cardholder data environment ii. Prior to hiring the personnel • Describe how it was observed that background checks are conducted: i. On potential personnel who will have access to cardholder data or the cardholder data environment ii. Prior to hiring the personnel		✓	✓	✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	**12.8** If the entity shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:						
12.8.1 Maintain a list of service providers.	**12.8.1** Verify that a list of service providers is maintained.	• Identify all service providers with whom cardholder data is shared. • Identify the document which includes a list of all service providers with whom cardholder data is shared. • 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.	**12.8.2** Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.	• For each service provider with whom cardholder data is shared: i. Identify the document that includes service provider acknowledgment of their responsibility for securing cardholder data.		✓			
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 were followed including proper due diligence prior to engaging any service provider.	• Identify the document that defines procedures for proper due diligence prior to engaging any service provider. • Describe how the procedures for proper due diligence were observed to be implemented.		✓		✓	
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.	• Identify the document that: i. Defines a program to monitor service providers' PCI DSS compliance status ii. Requires that service providers' PCI DSS compliance status be monitored at least annually • Describe how the program to monitor service providers' PCI DSS compliance status was observed to be implemented. • Describe how service providers' PCI DSS compliance status was observed to be monitored at least annually.		✓		✓	

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following:						
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: - Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business recovery and continuity procedures - Data back-up processes - Analysis of legal requirements for reporting compromises - Coverage and responses of all critical system components - Reference or inclusion of incident response procedures from the payment brands	**12.9.1.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	- Identify the incident response plan and procedure document(s). - Describe how the document includes: i. Roles and responsibilities ii. Communication strategies iii. Requirement for notification of the payment brands iv. Specific incident response procedures v. Business recovery and continuity procedures vi. Data back-up processes vii. Analysis of legal requirements for reporting compromises viii. Coverage for all critical system components ix. Responses for all critical system components x. Reference or inclusion of incident response procedures from the payment brands		✓			
	12.9.1.b Review documentation from a previously reported incident or alert to verify that the documented incident response plan and procedures were followed.	- Identify documentation from a previously reported incident or alert. - Describe how the documentation verifies that the defined incident response plan and procedures were followed.		✓			

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.9.2 Test the plan at least annually.	**12.9.2** Verify that the plan is tested at least annually.	• Identify the document that: i. Defines procedures for testing the incident response plan ii. Requires the plan be tested at least annually • Identify responsible personnel who were interviewed to confirm that: i. The incident response plan is tested according to the defined procedures. ii. The plan is tested at least annually. • Describe how it was observed that the incident response plan is: i. Tested according to the defined procedures ii. Tested at least annually		✓	✓	✓	
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.9.3** Verify through observation and review of policies, 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 that designates personnel to be available for: i. 24/7 incident monitoring ii. 24/7 incident response • Identify the document requiring 24/7 incident response and monitoring coverage for: i. Any evidence of unauthorized activity ii. Detection of unauthorized wireless access points iii. Critical IDS alerts iv. Reports of unauthorized critical system or content file changes • Describe how it was observed that 24/7 incident response and monitoring coverage is provided for: i. Evidence of unauthorized activity ii. Detection of unauthorized wireless access points iii. Critical IDS alerts iv. Reports of unauthorized critical system or content file changes		✓		✓	
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	**12.9.4** Verify through observation and review of policies that staff with responsibility for security-breach response are periodically trained.	• Identify the document requiring that staff with security breach responsibilities are periodically trained. • Describe how it was observed that staff with security breach responsibilities are periodically trained.		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	**12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.	• Identify the document that defines how the following are monitored: i. Alerts from intrusion-detection/intrusion-prevention ii. Alerts from file-integrity monitoring systems iii. Detection of unauthorized wireless access points • Identify the document that defines how the following are responded to: i. Alerts from intrusion-detection/intrusion-prevention ii. Alerts from file-integrity monitoring systems iii. Detection of unauthorized wireless access points • Describe how processes for monitoring the following were observed to be implemented: i. Alerts from intrusion-detection / intrusion-prevention ii. Alerts from file-integrity monitoring systems. iii. Detection of unauthorized wireless access points • Describe how processes for responding to the following were observed to be implemented: i. Alerts from intrusion-detection/intrusion-prevention ii. Alerts from file-integrity monitoring systems iii. Detection of unauthorized wireless access points		✓		✓	
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	• Identify the document which defines processes to modify and evolve the incident response plan: i. According to lessons learned ii. To incorporate industry developments • Describe how processes were observed to be implemented to modify and evolve the incident response plan: i. According to lessons learned ii. To incorporate industry developments		✓		✓	

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement A.1: Shared hosting providers must protect the cardholder data environment							
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. ***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below.						
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: • No entity on the system can use a shared web server user ID. • All CGI scripts used by an entity must be created and run as the entity's unique user ID.	• Identify whether the hosting provider allows hosted entities to run their own applications.				✓	
		If the hosting provider does not allow entities to run their own applications: • Identify the document which requires that entities must not run their own applications. • Describe how it was observed that hosted entities are not able to run their own applications.	✓	✓			

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	**Reporting Methodology**				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
		If the hosting provider does allow entities to run their own applications: • Identify the document which requires that application processes use a unique ID for each entity. • Identify the sample of: i. Servers ii. Hosted merchants and service providers (hosted entities) • For each item in the sample: i. Describe how the observed system configurations require that all hosted entities' application processes are run using the unique ID of that entity. ii. Describe how the hosted entities' application processes were observed to be running using unique IDs for each entity, including: ○ Entities on the system cannot use a shared web server user ID. ○ All CGI scripts used by an entity are created and run as the entity's unique user ID.	✓	✓		✓	✓
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	**A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin).	• Identify the document which requires that user IDs for hosted entities' application processes are not privileged users. • Identify the sample of: i. Servers ii. Hosted merchants and service providers (hosted entities) • For each item in the sample: i. Describe how the observed system configurations confirm that user IDs for hosted entities' application processes are not privileged users. ii. Describe how running application processes IDs were observed to not be privileged users.	✓	✓		✓	✓

PCI DSS Requirements	Testing Procedures	**ROC Reporting Details** (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
.	**A.1.2.b** Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.). ***Important:*** *An entity's files may not be shared by group*.	• Identify the document which defines permissions for hosted entities as follows: i. Read permissions are only assigned for the files and directories the hosted entity owns, or for necessary systems files. ii. Write permissions are only assigned for the files and directories the entity owns, or for necessary systems files. iii. Execute permissions are only assigned for the files and directories the hosted entity owns, or for necessary systems files. iv. Assigned permissions for hosted entities must be restricted (for example via file system permissions, access control lists, chroot, jailshell, etc.). v. An entity's files must not be shared by group. • Identify the sample of: i. Servers ii. Hosted merchants and service providers • For each item in the sample, describe how the system configurations were observed to assign permissions as follows: i. Read permissions are only assigned for the files and directories the hosted entity owns or for necessary systems files. ii. Write permissions are only assigned for the files and directories the hosted entity owns or for necessary systems files. iii. Execute permissions are only assigned for the files and directories the hosted entity owns or for necessary systems files. • For each item in the sample, describe how permissions were observed to be restricted (for example via file system permissions, access control lists, chroot, jailshell, etc.). • For each item in the sample, describe how it was observed that an entity's files are not shared by group.	✓	✓			✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	A.1.2.c Verify that an entity's users do not have write access to shared system binaries.	• Identify the document which requires that a hosted entity's users do not have write access to shared system binaries. • Identify the sample of: i. Servers ii. Hosted merchants and service providers • For each item in the sample, describe how observed system configurations ensure that hosted entities' users do not have write access to shared system binaries.	✓	✓			✓
	A.1.2.d Verify that viewing of log entries is restricted to the owning entity.	• Identify the document which requires that viewing of log entries is restricted to the owning entity. • Identify the sample of: i. Servers ii. Hosted merchants and service providers • For each item in the sample, describe how observed system configurations restrict viewing of log entries to the owning entity.	✓	✓			✓
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: • Disk space • Bandwidth • Memory • CPU	• Identify the document which defines restrictions for the use of i. Disk space ii. Bandwidth iii. Memory iv. CPU • Identify the sample of: i. Servers ii. Hosted merchants and service providers • For each item in the sample, describe how the observed system configurations implement restrictions for the use of: i. Disk space ii. Bandwidth iii. Memory iv. CPU	✓	✓			✓

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**A.1.3** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review by the owning entity. • Log locations are clearly communicated to the owning entity.	• Identify the document which requires that logging is enabled for each hosted entity environment. • Confirm that the document requires the following for each hosted entity environment: i. Logs are enabled for common third-party applications. ii. Logs are active by default. iii. Logs are available for review by the owning entity. iv. Log locations are clearly communicated to the owning entity • Identify the sample of: i. Servers ii. Hosted merchants and service providers • For each item in the sample, describe how it was observed that: i. Logging is enabled for each hosted entity. ii. Logs are enabled for common third-party applications. iii. Logs are active by default. iv. Logs are available for review by the owning entity. v. Log locations are clearly communicated to the owning entity. vi. Logging and audit trails are consistent with PCI DSS Requirement 10.	✓	✓		✓	✓
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.	• Identify the document which defines processes for timely forensics investigation in the event of a compromise to any hosted entity. • Identify the responsible personnel interviewed who confirm that processes are implemented in accordance with the document policies. • Describe how the processes were observed to be implemented to provide for timely forensics investigation in the event of a compromise to any hosted entity.		✓	✓	✓	