Payment Card Industry

Data Security Standard

PCI DSS v4.0.1 Report on Compliance Template

Revision 2

October 2024

Document Changes

Date	Version	Description
February 2014	PCI DSS 3.0, Revision 1.0	To introduce the template for submitting Reports on Compliance. This document is intended for use with version 3.0 of the PCI Data Security Standard.
July 2014	PCI DSS 3.0, Revision 1.1	Errata - Minor edits made to address typos and general errors, slight addition of content.
April 2015	PCI DSS 3.1, Revision 1.0	Revision to align with changes from PCI DSS 3.0 to PCI DSS 3.1 (see PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1 for details of those changes). Also includes minor edits made for clarification and/or format.
April 2016	PCI DSS 3.2, Revision 1.0	Revision to align with changes from PCI DSS 3.1 to PCI DSS 3.2 (see PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2 for details of those changes). Also includes minor corrections and edits made for clarification and/or format.
June 2018	PCI DSS 3.2.1 Revision 1.0	Revision to align with changes from PCI DSS 3.2 to PCI DSS 3.2.1 (see PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1 for details of changes). Also includes minor corrections and edits made for clarification and/or format.
March 2022	PCI DSS 4.0	Updates to align with the changes from PCI DSS v3.2.1 to PCI DSS v4.0 (see PCI DSS – Summary of Changes from PCI DSS Version 3.2.1 to 4.0 for details of changes). Also includes corrections and edits made for clarification and/or format.
December 2022	PCI DSS 4.0 Revision 1	Updates include minor clarifications, corrections to typographical errors, and removal of In Place with Remediation as a reporting option.
August 2024	PCI DSS 4.0.1	Updates to align with the changes from PCI DSS v4.0 to PCI DSS v4.0.1. See *PCI DSS – Summary of Changes from PCI DSS Version 4.0 to 4.0.1* for details of changes to PCI DSS and see *PCI DSS ROC Template – Summary of Changes from ROC Template v4.0 to v4.0.1* for details of changes to the ROC Template.
August 2024	PCI DSS v4.0.1 Revision 1	Correction to Assessment Findings selection options in Appendix A1 and A2 to remove duplicate columns. Added back inadvertently removed row of Assessment Finding selection options in Requirements 10.2.1.4, 10.2.1.5, 10.3.3, 12.1.4, and 12.6.3.2. Notes added or updated to align with notes in PCI DSS v4.0.1, where requirements are being replaced or superseded by new requirements after 31 March 2025.
October 2024	PCI DSS v4.0.1 Revision 2	In Appendix C and Appendix E, clarified heading for “Requirement Number and Definition”.

Table of Contents

ROC Template Instructions

This document, the PCI DSS v4.0.1 Report on Compliance Template ("ROC Template"), is the mandatory template for Qualified Security Assessors (QSAs) completing a Report on Compliance (ROC) for assessments against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*. The ROC Template provides the reporting instructions and template for QSAs to document PCI DSS assessments with the aim of ensuring a consistent level of reporting among assessors.

Use of this ROC Template is mandatory for all PCI DSS v4.0.1 submissions when documenting the results of a detailed PCI DSS assessment (as contrasted with a less detailed PCI DSS self-assessment documented in a Self-Assessment Questionnaire (SAQ)).

The tables in this template may be modified to increase/decrease the number of rows or to change the column width. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos to the title page below, is acceptable.

Do not delete any content from Part I or Part II of this document. The Instruction pages may be deleted; however, the assessor must follow these instructions while documenting the assessment. The addition of text or rows is acceptable, within reason, as noted above. Refer to the *PCI DSS v4.x Report on Compliance Template - Frequently Asked Questions* document on the PCI SSC website for further guidance.

The ROC is completed during PCI DSS assessments as part of an entity's validation process. The ROC provides details about the entity's environment and assessment methodology and documents the entity's assessment results for each PCI DSS requirement. A PCI DSS assessment involves thorough testing and assessment activities, from which the assessor will generate evidence (assessment 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 assessment. The ROC is a summary of evidence derived from the assessor's work papers to document how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the ROC provides a comprehensive summary of testing activities performed and information collected during the assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*. The information contained in a ROC must provide enough information and coverage to support the designated assessment findings.

ROC Sections

The ROC includes the following sections and appendices:

- Part I: Assessment Overview
  - Section 1: Contact Information and Summary of Results
  - Section 2: Business Overview
  - Section 3: Description of Scope of Work and Approach Taken
  - Section 4: Details about Reviewed Environment
  - Section 5: Quarterly Scan Results
- Part II: Sampling and Evidence, Findings and Observations
  - Section 6: Sampling and Evidence
  - Section 7: Findings and Observations
    - Build and Maintain a Secure Network and Systems
    - Protect Account Data
    - Maintain a Vulnerability Management Program
    - Implement Strong Access Control Measures
    - Regularly Monitor and Test Networks
    - Maintain an Information Security Policy
    - Appendix A: Additional PCI DSS Requirements
    - Appendix B: Compensating Controls
    - Appendix C: Compensating Controls Worksheet
    - Appendix D: Customized Approach
    - Appendix E: Customized Approach Template

Part I and Section 6 of Part II must be thoroughly and accurately completed to provide proper context for the Findings and Observations in Section 7 of Part II. The ROC Template includes tables with reporting instructions built-in to help assessors provide all required information throughout the document. Responses must be specific and focus on concise quality of detail, rather than lengthy, repeated verbiage. Use of template language for descriptions is discouraged and details must be specifically relevant to the assessed entity.

Assessment Findings

There are four possible assessment findings: In Place, Not Applicable, Not Tested, and Not in Place. At each sub-requirement there is a place to designate the result ("Assessment Findings"), which can be checked as appropriate. See the example format in *Figure 1*.

Refer to the following table when considering which selection to make. Only one assessment finding may be selected at the sub-requirement level and reporting associated with that assessment finding must be consistent across all required documents, including the AOC.

Refer to the *PCI DSS v4.x Report on Compliance Template - Frequently Asked Questions* document on the PCI SSC website for further guidance.

Assessment Finding	When to Use This Assessment Finding	Using Figure 1	Required Reporting
In Place	The expected testing has been performed, and all elements of the requirement have been met.	In *Figure 1*, the Assessment Finding at 1.1.1 is In Place if all report findings are In Place for 1.1.1.a and 1.1.1.b or a combination of In Place and Not Applicable.	Describe how the testing and evidence demonstrates the requirement is In Place.
Not Applicable	The requirement does not apply to the organization's environment. Not Applicable responses require reporting on testing performed to confirm the Not Applicable status including a detailed description explaining how it was determined that the requirement does not apply. Note that reporting instructions that start with "If Yes" or "If No" do not require additional testing to confirm the Not Applicable status. For example, if the Reporting Instruction was "If Yes, complete the following" and the response was "No" then the assessor would simply mark that section as Not Applicable or N/A and no further testing is required.	In *Figure 1*, the Assessment Finding at 1.1.1 is Not Applicable if both 1.1.1.a and 1.1.1.b are concluded to be Not Applicable. A requirement is applicable if any aspects of the requirement apply to the environment being assessed, and a Not Applicable designation in the Assessment Findings should not be used in this scenario. ***Note:*** *Requirements and/or individual bullets within a requirement noted as a best practice until its effective date are considered Not Applicable until the future date has passed. While it is true that the requirement is likely not tested (hence the original instructions), it is not required to be tested until the future date has passed, and the requirement is therefore not applicable until that date. As such, a Not Applicable response to future-dated requirements is accurate, whereas a Not Tested response would imply there was not any consideration as to whether it could apply.* *Once the effective date has passed, responses to those requirements should be consistent with instructions for all requirements.*	Describe the testing performed and the results of the testing that demonstrates the requirement is Not Applicable.

Assessment Finding	When to Use This Assessment Finding	Using Figure 1	Required Reporting
Not Tested	The requirement (or any single aspect of the requirement) was not included for consideration in the assessment and was not tested in any way. (See "What is the difference between Not Applicable and Not Tested?" in the following section for examples of when this option should be used.) ***Note**: Where Not Tested is used, the assessment is considered a Partial Assessment.*	In *Figure 1*, the Assessment Finding at 1.1.1 is Not Tested if either 1.1.1.a or 1.1.1.b are concluded to be Not Tested.	Describe why this requirement was excluded from the assessment.
Not in Place	Some or all elements of the requirement have not been met, are in the process of being implemented, or require further testing before it will be known if they are In Place. This response is also used if a requirement cannot be met due to a legal restriction, meaning that meeting the requirement would contravene a local or regional law or regulation. The assessor must confirm that a statutory law or regulation exists that prohibits the requirement from being met. ***Note:** Contractual obligations or legal advice are not legal restrictions.*	In *Figure 1*, the Assessment Finding at 1.1.1 is Not in Place if either 1.1.1.a or 1.1.1.b are concluded to be Not in Place.	Describe how the testing and evidence demonstrates the requirement is Not in Place. If the requirement is Not in Place due to a legal restriction, the assessor must describe the statutory law or regulation that prohibits the requirement from being met.

Method(s) Used

"Select If Below Method(s) was Used" is to designate if a compensating control or a customized approach (or both) was used to meet a requirement. See the example format in *Figure 1*.

It is possible for different aspects of a requirement to be met with a combination of these approaches. For example, if there are several types of system components that apply to a certain requirement, system component X may be met with a compensating control, while system component Y may be met as stated with the defined approach, and system component Z may be met with a customized approach.

Refer to the following table when considering whether to select one or both of these methods. If both methods were used for a sub-requirement, select both boxes; if neither method is used for a sub-requirement, do not select either box.

Refer to the *PCI DSS v4.x Report on Compliance Template - Frequently Asked Questions* document on the PCI SSC website for further guidance.

Method Used	When to Use Method	Using Figure 1	Required Reporting
Compensating Control	A compensating control has been implemented to meet some or all aspects of a requirement. The expected testing has been performed on the compensating control, and the Assessment Finding selected accurately represents the results of this testing. See *PCI DSS v4.x Appendices B and C* and the *PCI DSS v4.x Report on Compliance Template - Frequently Asked Questions* for details about compensating controls.	In *Figure 1*, "Compensating Control" is selected for Method Used if entity implemented a compensating control to meet this requirement. If both a compensating control and a customized approach were implemented to meet different aspects of a requirement, both items are selected.	Select the Compensating Control checkbox. Complete and include the Compensating Controls Worksheet in *Appendix C* (not pictured).
Customized Approach	A customized approach has been implemented to meet some or all aspects of a requirement. The assessor derived the appropriate testing procedures, performed that testing on the customized control, and the Assessment Finding selected accurately represents the results of this testing. ***Note:*** *Compensating controls are not an option for meeting the same aspect of a requirement that is met with a customized approach.* See *PCI DSS v4.x Section 8*, *PCI DSS v4.x Appendices D and E* and the *PCI DSS v4.x Report on Compliance Template - Frequently Asked Questions* for details about the customized approach.	In *Figure 1*, "Customized Approach" is selected for Method Used if entity implemented a customized approach to meet this requirement. If both a compensating control and a customized approach were implemented to meet different aspects of a requirement, both items are selected.	Select the Customized Approach checkbox. Complete and include the Customized Approach Template in *Appendix E* (not pictured).

Figure 1. Example Requirement

Requirement Description					
1.1 Example Requirement Description					
PCI DSS Requirement					
1.1.1 Example Requirement					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
1.1.1.a Example testing procedure	Example reporting instruction				
1.1.1.b Example testing procedure	Example reporting instruction				

What Is the Difference between Not Applicable and Not Tested?

Requirements that are Not Applicable to an environment must be verified as such. Using the example of wireless and an organization that does not use wireless technology in any capacity, an assessor could select Not Applicable for Requirements 1.3.3, 2.3.1–2.3.3, and 4.2.1.2 after the assessor confirms through testing that there are no wireless technologies used in their CDE or that connect to their CDE. Once this has been confirmed, the assessor may select Not Applicable for those specific requirements, and the accompanying reporting must reflect the testing performed to confirm the Not Applicable status.

If a requirement is completely excluded from review without any consideration as to whether it could apply, the Not Tested option must be selected. Examples of situations where this could occur may include:

- An organization may be asked by their acquirer or brand to validate a subset of requirements—for example, using the PCI DSS Prioritized Approach to validate certain milestones.
- An organization may want to validate a new security control that impacts only a subset of requirements—for example, implementation of a new encryption method that requires assessment of PCI DSS Requirements 2, 3, and 4.
- A service provider organization might offer a service that covers only a limited number of PCI DSS requirements—for example, a physical storage provider may want to validate only the physical security controls per PCI DSS Requirement 9 for their storage facility.

In these scenarios, the organization wants to validate only certain PCI DSS requirements, even though other requirements might also apply to their environment.

Items marked as Not Applicable require that the assessor render an opinion that the item is not applicable; however, with Not Tested, the assessor is simply following the entity's instructions to not test something with no opinion needed from the assessor.

The resulting ROC (in section 1.8.1) and AOC(s) (in Part 2g: Summary of Assessment) must indicate which if any requirements were Not Applicable or Not Tested.

Dependence on Another Service Provider's Compliance

Generally, when reporting on a requirement where a third-party service provider is responsible for the task(s), the response is minimally captured at each requirement in the "Describe why the assessment finding was selected" section and the corresponding evidence is identified in the evidence section of the requirement. An acceptable response for an In Place finding for 1.1.1.a would be documented at the requirement and may be something like:

> *Assessor verified this is the responsibility of Service Provider X, as verified through review of x/y contract (document). Assessor reviewed the AOC for Service Provider X, dated YYYY-MM-DD, and confirmed the service provider was found to be PCI DSS compliant against PCI DSS vX.X for all applicable requirements, and that it covers the scope of the services used by the assessed entity.*

That response could vary, but what's important is that it is noted as In Place, and that there has been a level of testing by the assessor to support the conclusion that this responsibility is verified and that the responsible party has been tested against the requirement and found to be compliant.

Understanding the Reporting Instructions

The reporting instructions in the ROC Template explain the intent of the response required. Responses should be specific and relevant to the assessed entity. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage and should avoid generic templated language.

Assessor responses generally fall into categories, such as the following:

Reporting Instruction Term	Example Usage	Description of Response
Indicate	Indicate whether the assessed entity is an issuer or supports issuing services.	The response would be either "Yes" or "No" as shown: ☐ Yes ☐ No ***Note**: The applicability of some reporting instructions may be dependent on the response of a previous reporting instruction. If applicable, the reporting instruction will direct the assessor to a subsequent instruction based on the yes/no answer.*
Identify	Identify the evidence reference number(s) from Section 6 for all documentation examined for this testing procedure.	The response would include the relevant item(s) requested. Example Reporting Instruction: "Identify the evidence reference number(s) from Section 6 for all documentation examined for this testing procedure." Example Response: Doc-01 OR Doc-01 (Company XYZ Information Security Policy) ***Note:** When a reference number is available, it is required; however, the assessor also has the option to list individual items in addition to the reference number.*
Describe	Describe why the assessment finding was selected.	The response would include a detailed description of the item or activity in question — for example, details of how the evidence examined or individuals interviewed demonstrate a requirement was met, or how the assessor concluded a control implemented is fit-for-purpose. The response should be of sufficient detail to provide the reader with a comprehensive understanding of the item or activity being described.
Attest	Identify the name of the QSA who attests.	The assessor's name is simply provided in the response. This "signature" adds more weight than a simple "yes" or "checkmark" response and is used when no additional reporting is needed.

Dos and Don'ts: Reporting Expectations

DO:	DON'T:
• Use this Reporting Template when assessing to PCI DSS 4.0.1. • Provide a completed *Appendix C Compensating Control Worksheet* for any requirement met with a compensating control. • Provide a completed *Appendix E Customized Approach Template* for any requirement met with a customized approach. • Read and understand the intent of each Requirement and Testing Procedure. • Read the PCI DSS Applicability Notes and Guidance column for each requirement (in the Standard). • Provide a response for every Testing Procedure. • Provide sufficient detail and information to thoroughly document the assessment. • Ensure sufficient detail and information are included in the workpaper evidence. • Ensure all parts of the Testing Procedure and Reporting Instruction are addressed. • Ensure the response covers all applicable system components, business functions, or facilities. • Perform an internal quality assurance review of the ROC for clarity, accuracy, and quality. • Provide useful, meaningful diagrams as directed.	• Do not select the In Place response without verification that the requirement is met (plans to meet a requirement in the future do not warrant an In Place response) • Do not copy responses from one requirement to another without first confirming that the response is fully applicable to each requirement. • Do not copy responses from previous assessments. • Do not include information irrelevant to the assessment. • Do not leave any spaces blank. If a section does not apply, annotate it as such.

PCI DSS v4.0.1 Report on Compliance Template

Complete the following ROC Template per these instructions. The following title page can be populated according to the assessor company's corporate document guidelines (for example, company name, logo, date, version, etc.). All instructional content (this page and all preceding pages) may be deleted by the assessor prior to finalizing the report.

PCI DSS v4.0.1 Report on Compliance

Entity Name:

Date of Report:

Date Assessment Ended:

Part I Assessment Overview

1 Contact Information and Summary of Results

1.1 Contact Information

Assessed Entity	
Company name:	
DBA (doing business as):	
Mailing address:	
Company main website:	
Contact name:	
Contact title:	
Contact phone number:	
Contact e-mail address:	
Assessed Entity Internal Security Assessors	
Identify all Internal Security Assessors (ISAs) involved in the assessment. If there were none, mark as Not Applicable. (Add rows as needed)	
ISA name:	
Qualified Security Assessor Company	
Company name:	
Mailing address:	
Company website:	

Lead Qualified Security Assessor	
Lead Assessor name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Additional Assessors	
Identify all Associate QSAs involved in the assessment. If there were none, mark as Not Applicable. (Add rows as needed)	
Associate QSA name:	Associate QSA mentor name:
Identify all other assessors involved in the assessment. If there were none, mark as Not Applicable. (Add rows as needed)	
Assessor name:	Assessor certificate number:

Assessor Quality Assurance (QA) Primary Reviewer for this specific report (not the general QA contact for the QSA Company)	
QA reviewer name:	
QA reviewer phone number:	
QA reviewer e-mail address:	
QA reviewer's PCI credentials or certificate number: (See the current QSA Qualification Requirements for acceptable credentials)	

1.2 Date and Timeframe of Assessment

Date of Report: ***Note:*** *The "Date of Report" indicates the completion date of the ROC, and therefore must be no earlier than the date on which the QSA Company and assessed entity agree on the final version of the ROC.*	
Date assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	
Date assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	
Identify the date(s) spent onsite at the assessed entity.	

1.3 Remote Assessment Activities

Refer to the *PCI SSC Remote Assessment Guidelines and Procedures* on the PCI SSC website for more information.

To what extent were remote testing methods used for this assessment?	☐ All testing was performed onsite ☐ A combination of onsite and remote testing methods was used ☐ All testing was performed remotely
If remote testing was used for any part of the assessment, briefly describe why onsite testing was not feasible or practical.	

1.4 Additional Services Provided by QSA Company

The *PCI SSC Qualification Requirements for Qualified Security Assessors (QSA)* includes content on "Independence," which specifies requirements for assessor disclosure of services and/or offerings that could reasonably be viewed to affect the independence of assessment. Complete the section below after reviewing the relevant portions of the Qualification Requirements to ensure responses are consistent with documented obligations.

Indicate whether the QSA Company provided any consultation on the development or implementation of controls used for the Customized Approach. ***Note**: This does not apply to the assessment of the Customized Approach.*	☐ Yes ☐ No
If "**Yes**," describe the nature of the consultation.	
Disclose all products or services provided to the assessed entity by the QSA Company that are not listed above and that were reviewed during this assessment or could reasonably be viewed to affect independence of assessment.	
Describe efforts made to ensure no conflict of interest resulted from the above-mentioned products and services provided by the QSA Company.	

1.5 Use of Subcontractors

Indicate whether any assessment activities were subcontracted to another Assessor Company. ***Note:*** *The use of subcontractors must conform with the requirements defined in the Qualification Requirements for Qualified Security Assessors (QSA) and Qualified Security Assessor Program Guide.*	☐ Yes ☐ No
If yes, identify the Assessor Company(s) utilized during the assessment.	

1.6 Additional Information/Reporting

Identify the number of consecutive years (including the current year) the QSA Company has issued ROCs for this entity.	

1.7 Overall Assessment Result

Indicate below whether a full or partial assessment was completed. Select only one.

☐	**Full Assessment:** All requirements have been assessed and therefore no requirements were marked as Not Tested.
☐	**Partial Assessment:** One or more requirements have not been assessed and were therefore marked as Not Tested. Any requirement not assessed is noted as Not Tested in section 1.8.1 below.

Overall Assessment Result (Select only one)	
☐	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT rating; thereby the assessed entity has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating; thereby the assessed entity has not demonstrated compliance with PCI DSS requirements.
☐	**Compliant but with Legal Exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating, thereby the assessed entity has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

1.8 Summary of Assessment

1.8.1 Summary of Assessment Findings and Methods

Indicate all the findings and assessment methods within each PCI DSS principal requirement. Select all that apply. For example, ***In Place*** and ***Not Applicable*** must both be selected for Requirement 1 if there is at least one sub-requirement marked ***In Place*** and one sub-requirement marked ***Not Applicable***. The columns for Compensating Controls and Customized Approach must be selected if there is at least one sub-requirement within the principal requirement that utilizes the respective method. For example, Compensating Control and Customized Approach must both be checked if at least one sub-requirement utilizes Compensating Controls and at least one sub requirement utilizes a Customized Approach. If neither Compensating Controls nor Customized Approach are used, then leave both blank.

PCI DSS Requirement	Assessment Finding Select all options that apply.				Select If Below Method(s) Was Used	
	In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control**	**Customized Approach**
Requirement 1:	☐	☐	☐	☐	☐	☐
Requirement 2:	☐	☐	☐	☐	☐	☐
Requirement 3:	☐	☐	☐	☐	☐	☐
Requirement 4:	☐	☐	☐	☐	☐	☐
Requirement 5:	☐	☐	☐	☐	☐	☐
Requirement 6:	☐	☐	☐	☐	☐	☐
Requirement 7:	☐	☐	☐	☐	☐	☐
Requirement 8:	☐	☐	☐	☐	☐	☐
Requirement 9:	☐	☐	☐	☐	☐	☐
Requirement 10:	☐	☐	☐	☐	☐	☐
Requirement 11:	☐	☐	☐	☐	☐	☐
Requirement 12:	☐	☐	☐	☐	☐	☐

PCI DSS Requirement	Assessment Finding Select all options that apply.				Select If Below Method(s) Was Used	
	In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control**	**Customized Approach**
Appendix A1:	☐	☐	☐	☐	☐	☐
Appendix A2:	☐	☐	☐	☐	☐	☐
Appendix A3:	☐	☐	☐	☐	☐	☐

In the sections below identify the sub-requirements with the following results and assessment methods. If there are none, enter "Not Applicable."

Note: *Natural grouping of requirements is allowed (for example, Req. 3, 1.1, 1.1.1, 1.1.2, or 1.2.1 through 1.2.3, etc.) to reduce the number of individual requirements listed.*

Not Applicable	**Not Tested**	**Not in Place Due to a Legal Restriction**	**Not in Place Not Due to a Legal Restriction**	**Compensating Control**	**Customized Approach**

2 Business Overview

2.1 Description of the Entity's Payment Card Business

Provide an overview of the entity's payment card business, including:

Describe the nature of the entity's business (what kind of work they do, etc.). ***Note**: This is not intended to be a cut-and-paste from the entity's website but should be a tailored description that shows the assessor understands the business of the entity being assessed.*	
Describe the entity's business, services, or functions that store, process, or transmit account data.	
Describe any services or functions that the entity performs that could impact the security of account data. (For example, merchant web site payment redirects or if the entity provides managed services)	
Identify the payment channels the entity utilizes.	☐ Card-Present ☐ Mail Order/Telephone Order (MOTO) ☐ E-Commerce
Other details, if applicable:	

3 Description of Scope of Work and Approach Taken

3.1 Assessor's Validation of Defined Scope Accuracy

Describe how the assessor validated the accuracy of the defined PCI DSS scope for the assessment:

As noted in *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*: "The minimum steps for an entity to confirm the accuracy of their PCI DSS scope are specified in PCI DSS Requirement 12.5.2. The entity is expected to retain documentation to show how PCI DSS scope was determined. The documentation is retained for assessor review and for reference during the entity's next PCI DSS scope confirmation activity. For each PCI DSS assessment, the assessor validates that the scope of the assessment is accurately defined and documented."

Describe how the assessor's evaluation of scope differs from the assessed entity's evaluation of scope as documented in Requirement 12.5. If no difference was identified, mark as "Not Applicable."	
Provide the name of the assessor who attests that: • They have performed an independent evaluation of the scope of the assessed entity's PCI DSS environment. • If the assessor's evaluation identified areas of scope not included in the assessed entity's documented scope, the assessed entity has updated their scoping documentation. • The scope of the assessment is complete and accurate to the best of the assessor's knowledge.	
Describe any business functions, locations, payment channels, or other areas of scope that were excluded from the assessment including the following: • What was excluded. • Why was it excluded. • If it was included in a separate assessment. If none, mark as "Not Applicable."	
Identify any factors that resulted in reducing or limiting scope (for example, segmentation of the environment, use of a P2PE solution, etc.) If none, mark as "Not Applicable."	

Describe any use of SAQ eligibility criteria in determining applicability of PCI DSS requirements for this assessment, including the following: • The type of SAQ applied. • The eligibility criteria for the applicable SAQ. • How the assessor verified that the assessed entity's environment meets the eligibility criteria. If not used mark as "Not Applicable." *Note: The only SAQ for service providers is SAQ D for Service Providers. All other SAQs are for merchants only.*	
Additional information, if applicable:	

3.2 Segmentation

Indicate whether the assessed entity has used segmentation to reduce the scope of the assessment. ***Note:*** *An environment with no segmentation is considered a "flat" network where all systems are considered to be in scope.*	☐ Yes ☐ No
• If "No," provide the name of the assessor who attests that the entire network has been included in the scope of the assessment.	
• If "Yes," complete the following:	
– Describe how the segmentation is implemented, including the technologies and processes used.	
– Describe the environments that were confirmed to be out of scope as a result of the segmentation methods.	
– Provide the name of the assessor who attests that the segmentation was verified to be adequate to reduce the scope of the assessment AND that the technologies/processes used to implement segmentation were included in this PCI DSS assessment.	

3.3 PCI SSC Validated Products and Solutions

For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (For example: 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption [P2PE] solutions, Software-Based PIN Entry on COTS [SPoC] solutions, Contactless Payments on COTS [CPoC] solutions, and Mobile Payment on COTS [MPoC] products.)

Indicate whether the assessed entity uses one or more PCI SSC validated products or solutions.	☐ Yes ☐ No
If "**Yes**," provide the following information regarding items the organization uses from PCI SSC's Lists of Validated Products and Solutions:	

Name of PCI SSC validated product or solution	Version of product or solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing

Provide the name of the assessor who attests that they have read the instruction manual associated with each of the software/solution(s) listed above and confirmed that the merchant has implemented the solution per the instructions and detail in the instruction manual.	
Any additional comments or findings the assessor would like to include, if applicable.	

4 Details About Reviewed Environments

4.1 Network Diagrams

Provide one or more network diagrams that:

- Shows all connections between the CDE and other networks, including any wireless networks.
- Is accurate and up to date with any changes to the environment.
- Illustrates all network security controls that are defined for connection points between trusted and untrusted networks.
- Illustrates how system components storing cardholder data are not directly accessible from the untrusted networks.
- Includes the techniques (such as intrusion-detection systems and/or intrusion-prevention systems) that are in place to monitor all traffic:
  - At the perimeter of the cardholder data environment.
  - At critical points in the cardholder data environment.

Insert Diagrams

4.2 Account Dataflow Diagrams

Provide one or more dataflow diagrams that:

- Shows all account data flows across systems and networks.
- Are accurate and up to date.

Insert Diagrams

4.2.1 Description of Account Data Flows

Identify in which of the following account data flows the assessed entity participates: ***Note:*** *These data flows must be described in detail in the sections of the table that follow.*
☐ Authorization ☐ Capture ☐ Settlement ☐ Chargeback/Dispute ☐ Refunds ☐ Other

Identify and describe all data flows. Descriptions should include how and where account data enters the environment, is transmitted, is processed, is stored, and how and why any personnel access the account data. Add rows as necessary.

Account data flows (For example, account data flow 1, account data flow 2)	Description (Include the type of account data)

4.3 Storage of Account Data

Identify all databases, tables, and files storing account data and provide the following details:

Note: *The list of files and tables that store account data in the table below must be supported by an inventory created (or obtained from the assessed entity) and retained by the assessor in the workpapers.*

Data Store[1]	File Name(s), Table Names(s) and/or Field Names	Account Data Elements Stored[2]	How Data Is Secured[3]	How Access to Data Stores Is Logged[4]

1 Database name, file server name, and so on.
2 For example, PAN, expiry, cardholder name, and so on.
3 For example, what type of encryption and strength.
4 Description of logging mechanism used for logging access to data—for example, describe the enterprise log management solution, application-level logging, operating system logging, etc. in place

4.3.1 Storage of SAD

If SAD is stored complete the following: ***Note:*** *Anywhere SAD is stored should be documented in the table in 4.3*	
Indicate whether SAD is stored post authorization:	☐ Yes ☐ No
Indicate whether SAD is stored as part of Issuer functions:	☐ Yes ☐ No

4.4 In-Scope Third-Party Service Providers (TPSPs)

Provide the following for each third-party service provider:

Refer to PCI DSS v4.x, section 4 Scope of PCI DSS Requirements, subsection Use of Third-Party Service Providers for more information.

Company Name	Identify what account data is shared or, if account data is not shared, how the organization could impact the security of account data[1]	Describe the purpose for utilizing the service provider[2]	Has the third party been assessed separately against PCI DSS?		If Yes, identify the date and PCI DSS version of the AOC.		If No, were the services provided by the third party included in this assessment?	
			Yes	No	Date	Version	Yes	No
			☐	☐			☐	☐
			☐	☐			☐	☐
			☐	☐			☐	☐
			☐	☐			☐	☐
			☐	☐			☐	☐

1 For example, PAN, expiry date, providing support via remote access, and so on.
2 For example, third-party storage, transaction processing, custom software development, and so on.

4.5 In-Scope Networks

Identify all in-scope networks including the type of network (for example, wired, Wi-Fi, cloud, etc.).

Note: *This section must align with networks identified on the network diagram.*

Describe all networks that store, process, and/or transmit Account Data:

Network Name (In scope)	Type of Network	Function/ Purpose of Network

Describe all networks that do not store, process, and/or transmit Account Data but are still in scope—for example, connected to the CDE or provide management functions to the CDE, etc.:

Network Name (In Scope)	Type of Network	Function/Purpose of Network

4.6 In-Scope Locations/Facilities

Identify and provide details for all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers and mail rooms) in scope. Add rows, as needed.

Facility Type (Datacenters, corporate office, call center, mail processing facility, etc.)	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (for example, city, country)
Example 1: Data center	*1*	*Los Angeles, California, United States*
Example 2: retail locations	*132*	*92 locations in the United States and 40 in Canada*

4.7 In-Scope System Component Types

Identify all types of system components in scope. Refer to PCI DSS v4.x section *4 Scope of PCI DSS Requirements* for examples, that include but are not limited to, of system component types that are in scope for PCI DSS requirements.

For each item, even if they reside with other system components, list them below with each component with different roles, vendors, or make/model/version on separate rows. Add rows as needed.

Type of System Component[1]	Total Number of System Components[2]	Vendor	Product Name and Version	Role/Function Description

1 For example, application, firewall, server, IDS, Anti-malware software, database, and so on.

2 How many system components of this type are in scope.

5 Quarterly Scan Results

5.1 Quarterly External Scan Results

Identify each quarterly ASV scan performed within the last 12 months in the table below. Refer to PCI DSS Requirement 11.3.2 for information about initial PCI DSS assessments against the ASV scan requirements.

Date of the Scan(s)	Name of ASV that Performed the Scan	Were any vulnerabilities found that resulted 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
		Yes	**No**	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Indicate whether this is the assessed entity's initial PCI DSS assessment against the ASV scan requirements.	☐ Yes ☐ No
If **yes**, Identify the name of the document the assessor verified to include the entity's documented policies and procedures requiring scanning at least once every three months going forward.	
Assessor comments, if applicable:	

5.2 Attestations of Scan Compliance

The scans must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the PCI DSS Approved Scanning Vendors (ASV) Program Guide.

Indicate whether the ASV and the assessed entity 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.	☐ Yes ☐ No

5.3 Quarterly Internal Scan Results

In the table below identify each quarterly internal vulnerability scan performed within the last 12 months.

Date of the Scan(s)	Was the scan performed via authenticated scanning?		Were any high-risk or critical vulnerabilities per the entity's vulnerability risk rankings at Requirement 6.3.1 found?		For all scans where high-risk or critical vulnerabilities were found, provide date(s) of re-scans showing that the vulnerabilities have been corrected.
	Yes	**No**	**Yes**	**No**	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	

Indicate if this is the assessed entity's initial PCI DSS assessment against the internal scan requirements.	☐ Yes ☐ No
If **yes**, Identify the name of the document the assessor verified to include the entity's documented policies and procedures requiring scanning at least once every three months going forward.	
Assessor comments, if applicable:	

Part II Sampling and Evidence, Findings and Observations

6 Sampling and Evidence

6.1 Evidence Retention

Describe the repositories where the evidence collected during this assessment is stored including the names of the repositories and how the data is secured.	
Identify the entity or entities who controls the evidence repositories.	
Indicate whether the entity or entities in control of the evidence repositories understands that all evidence from this assessment must be maintained for a minimum of 3 years and must be made available to PCI SSC upon request.	☐ Yes ☐ No
Identify the assessor who attests that all evidence, including interview notes, system configuration evidence, documentation, and observation notes has been gathered and stored as per the QSA Company's evidence retention policy.	

6.2 Sampling

Indicate whether sampling is used.	☐ Yes ☐ No
• If "No," provide the name of the assessor who attests that every item in each population has been assessed.	
• If "Yes," complete the following: ***Note**: If multiple sampling methodologies are used, clearly respond for each methodology.*	
– Describe the sampling rationale(s) used for selecting sample sizes (for people, process evidence, technologies, devices, locations/sites, etc.).	
– Describe how the samples are appropriate and representative of the overall populations.	
– Indicate whether standardized processes and controls are in place that provide consistency between each item in the samples—for example, automated system build processes, configuration change detection, etc. o If "**Yes**," describe how the processes and controls were validated by the assessor to be in place and effective.	☐ Yes ☐ No

6.3 Sample Sets for Reporting

Identify all sample sets used during testing. This table only needs to be completed for populations where sampling was used.

When sampling is used the assessor must identify the items in the population that were tested (for example, as "Sample Set-1") as part of the sample in the table below. All unique sample sets must be documented in this table.

Note: *For items where the total population fluctuates or is difficult to determine, the assessor may work with the assessed entity to provide an estimated total population in the total population column below.*

Tested Sample Set Reference Number	Sample Type/ Description[1]	Identify All Items in the Sample Set[2]	Selection Method[3]	Total Sampled	Total Population

1 For example, firewalls, datacenters, change records, User IDs, and so on.
2 For example, unique system identifiers, location addresses/identifiers, change record numbers/identifiers, personnel identifier, and so on.
3 Describe the method for selecting individual items in the sample sets.

6.4 Documentation Evidence

Identify all evidence for any testing procedure requiring a review of documents such as policies, procedures, standards, records, inventories, vendor documentation, and diagrams. Include the following: (Add rows as needed)

Reference Number	Document Name (including version, if applicable)	Document Purpose	Document Revision Date (if applicable)
EXAMPLE: Doc-1	*Company XPY Information Security Policy*	*Information Security Policy*	*2021-02-18*

6.5 Interview Evidence

Identify all evidence for testing procedures requiring an interview, such as interview notes. Include the following: (Add rows as needed)

Reference Number	Title of Workpaper with Interview Notes	Topics Covered	Role(s) of Interviewee(s)
EXAMPLE: Int-01	*Assessor notes from interview with Information Security Manager*	*Information security processes including security vulnerability risk ranking, anti-malware configurations, and cryptographic key management.*	*Information Security Manager*

6.6 Other Assessment Evidence

Identify evidence for any testing procedure that requires observation of processes or examination of system evidence, such as review of configurations, settings, audit logs, access control lists, etc. Include the following: (Add rows as needed.)

Reference Number	Title of Workpaper or Evidence	Topics Covered or Evidence Collected	Sample Set Reference Number from Table 6.3 (if applicable)
EXAMPLE: Evidence-1	*Windows Config-1*	*Configuration settings for: Passwords, Logging, Services and Protocols.*	*Sample Set 1*

7 Findings and Observations

Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

Requirement Description
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.

PCI DSS Requirement
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 1 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.					
Assessment Findings (select one)				Select if below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
1.1.2.b Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
1.2 Network security controls (NSCs) are configured and maintained.

PCI DSS Requirement
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.2.1.a Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration standards** examined for this testing procedure.	
1.2.1.b Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.	

PCI DSS Requirement
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.2.2.a Examine documented procedures to verify that changes to network connections and configurations of NSCs are included in the formal change control process in accordance with Requirement 6.5.1.	**Identify** the evidence reference number(s) from Section 6 for all **documented procedures** examined for this testing procedure.	
1.2.2.b Examine network configuration settings to identify changes made to network connections. Interview responsible personnel and examine change control records to verify that identified changes to network connections were approved and managed in accordance with Requirement 6.5.1.	**Identify** the evidence reference number(s) from Section 6 for all **network configuration settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **change control records** examined for this testing procedure.	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.2.2.c Examine network configuration settings to identify changes made to configurations of NSCs. Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1.	**Identify** the evidence reference number(s) from Section 6 for all **network configuration settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **change control records** examined for this testing procedure.	

PCI DSS Requirement					
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
1.2.3.a Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **diagrams** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **network configurations** examined for this testing procedure.				
1.2.3.b Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
1.2.4.a Examine data-flow diagram(s) and interview personnel to verify the diagram(s) show all account data flows in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **data-flow diagram(s)** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
1.2.4.b Examine documentation and interview responsible personnel to verify that the data-flow diagram(s) is accurate and updated when there are changes to the environment.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
1.2.5.a Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
1.2.5.b Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.				

PCI DSS Requirement					
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
1.2.6.a Examine documentation that identifies all insecure services, protocols, and ports in use to verify that for each, security features are defined to mitigate the risk.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
1.2.6.b Examine configuration settings for NSCs to verify that the defined security features are implemented for each identified insecure service, protocol, and port.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.				

PCI DSS Requirement					
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.2.7.a Examine documentation to verify procedures are defined for reviewing configurations of NSCs at least once every six months.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
1.2.7.b Examine documentation of reviews of configurations for NSCs and interview responsible personnel to verify that reviews occur at least once every six months.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
1.2.7.c Examine configurations for NSCs to verify that configurations identified as no longer being supported by a business justification are removed or updated.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	

PCI DSS Requirement					
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
1.2.8 Examine configuration files for NSCs to verify they are in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration files** examined for this testing procedure.				

Requirement Description
1.3 Network access to and from the cardholder data environment is restricted.

PCI DSS Requirement
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.3.1.a Examine configuration standards for NSCs to verify that they define restricting inbound traffic to the CDE is in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration standards** examined for this testing procedure.	
1.3.1.b Examine configurations of NSCs to verify that inbound traffic to the CDE is restricted in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	

PCI DSS Requirement					
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
1.3.2.a Examine configuration standards for NSCs to verify that they define restricting outbound traffic from the CDE in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration standards** examined for this testing procedure.				
1.3.2.b Examine configurations of NSCs to verify that outbound traffic from the CDE is restricted in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.				

PCI DSS Requirement
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.3.3 Examine configuration settings and network diagrams to verify that NSCs are implemented between all wireless networks and the CDE, in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **network diagrams** examined for this testing procedure.	

Requirement Description
1.4 Network connections between trusted and untrusted networks are controlled.

PCI DSS Requirement
1.4.1 NSCs are implemented between trusted and untrusted networks.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.4.1.a Examine configuration standards and network diagrams to verify that NSCs are defined between trusted and untrusted networks.	**Identify** the evidence reference number(s) from Section 6 for all **configuration standards** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **network diagrams** examined for this testing procedure.	
1.4.1.b Examine network configurations to verify that NSCs are in place between trusted and untrusted networks, in accordance with the documented configuration standards and network diagrams.	**Identify** the evidence reference number(s) from Section 6 for all **network configurations** examined for this testing procedure.	

PCI DSS Requirement
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.4.2 Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	

PCI DSS Requirement					
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.4.3 Examine vendor documentation and configurations for NSCs to verify that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	

PCI DSS Requirement					
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.4.4.a Examine the data-flow diagram and network diagram to verify that it is documented that system components storing cardholder data are not directly accessible from the untrusted networks.	**Identify** the evidence reference number(s) from Section 6 for all **data-flow diagram** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **network diagram** examined for this testing procedure.	
1.4.4.b Examine configurations of NSCs to verify that controls are implemented such that system components storing cardholder data are not directly accessible from untrusted networks.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	

PCI DSS Requirement					
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.4.5.a Examine configurations of NSCs to verify that the disclosure of internal IP addresses and routing information is limited to only authorized parties.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	
1.4.5.b Interview personnel and examine documentation to verify that controls are implemented such that any disclosure of internal IP addresses and routing information is limited to only authorized parties.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

Requirement Description
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

PCI DSS Requirement
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.5.1.a Examine policies and configuration standards and interview personnel to verify security controls for computing devices that connect to both untrusted networks, and the CDE, are implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies** examined for this testing procedure.	
(continued on next page	**Identify** the evidence reference number(s) from Section 6 for all **configuration standards** examined for this testing procedure.	

***1.5.1.a** (continued)*	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**
1.5.1.b Examine configuration settings on computing devices that connect to both untrusted networks and the CDE to verify settings are implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.	

Requirement 2: Apply Secure Configurations to All System Components

Requirement Description
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.

PCI DSS Requirement
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 2 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 2 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
2.1.2.b Interview personnel with responsibility for performing activities in Requirement 2 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
2.2 System components are configured and managed securely.

PCI DSS Requirement
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.2.1.a Examine system configuration standards to verify they define processes that include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration standards** examined for this testing procedure.	

2.2.1.b Examine policies and procedures and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.3.1.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
2.2.1.c Examine configuration settings and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before or immediately after a system component is connected to a production environment.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement

2.2.2 Vendor default accounts are managed as follows:

- If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.
- If the vendor default account(s) will not be used, the account is removed or disabled.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.2.2.a Examine system configuration standards to verify they include managing vendor default accounts in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration standards** examined for this testing procedure.	
2.2.2.b Examine vendor documentation and observe a system administrator logging on using vendor default accounts to verify accounts are implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations** conducted for this testing procedure.	
2.2.2.c Examine configuration files and interview personnel to verify that all vendor default accounts that will not be used are removed or disabled.	**Identify** the evidence reference number(s) from Section 6 for all **configuration files** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.2.3.a Examine system configuration standards to verify they include managing primary functions requiring different security levels as specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration standards** examined for this testing procedure.	
2.2.3.b Examine system configurations to verify that primary functions requiring different security levels are managed per one of the ways specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

2.2.3.c Where virtualization technologies are used, examine the system configurations to verify that system functions requiring different security levels are managed in one of the following ways: • Functions with differing security needs do not co-exist on the same system component. • Functions with differing security needs that exist on the same system component are isolated from each other. • Functions with differing security needs on the same system component are all secured to the level required by the function with the highest security need.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

PCI DSS Requirement					
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.2.4.a Examine system configuration standards to verify necessary services, protocols, daemons and functions are identified and documented.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration standards** examined for this testing procedure.	
2.2.4.b Examine system configurations to verify the following: • All unnecessary functionality is removed or disabled. • Only required functionality, as documented in the configuration standards, is enabled.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

PCI DSS Requirement					
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
2.2.5.a If any insecure services, protocols, or daemons are present, examine system configuration standards and interview personnel to verify they are managed and implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration standards** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
2.2.5.b If any insecure services, protocols, or daemons, are present, examine configuration settings to verify that additional security features are implemented to reduce the risk of using insecure services, daemons, and protocols.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.				

PCI DSS Requirement
2.2.6 System security parameters are configured to prevent misuse.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.2.6.a Examine system configuration standards to verify they include configuring system security parameters to prevent misuse.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration standards** examined for this testing procedure.	
2.2.6.b Interview system administrators and/or security managers to verify they have knowledge of common security parameter settings for system components.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
2.2.6.c Examine system configurations to verify that common security parameters are set appropriately and in accordance with the system configuration standards.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

PCI DSS Requirement					
2.2.7 All non-console administrative access is encrypted using strong cryptography.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.2.7.a Examine system configuration standards to verify they include encrypting all non-console administrative access using strong cryptography.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration standards** examined for this testing procedure.	
2.2.7.b Observe an administrator log on to system components and examine system configurations to verify that non-console administrative access is managed in accordance with this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **observations of administrator log on(s)** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

2.2.7.c Examine settings for system components and authentication services to verify that insecure remote login services are not available for non-console administrative access.	**Identify** the evidence reference number(s) from Section 6 for all **settings for system components and authentication services** examined for this testing procedure.	
2.2.7.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
2.3 Wireless environments are configured and managed securely.

PCI DSS Requirement
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
2.3.1.a Examine policies and procedures and interview responsible personnel to verify that processes are defined for wireless vendor defaults to either change them upon installation or to confirm them to be secure in accordance with all elements of this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

2.3.1.b Examine vendor documentation and observe a system administrator logging into wireless devices to verify: • SNMP defaults are not used. • Default passwords/passphrases on wireless access points are not used.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for the **observations of administrator log in(s)** for this testing procedure.	
2.3.1.c Examine vendor documentation and wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **wireless configuration settings** examined for this testing procedure.	

PCI DSS Requirement					
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
2.3.2 Interview responsible personnel and examine key-management documentation to verify that wireless encryption keys are changed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **key-management documentation** examined for this testing procedure.				

Protect Account Data

Requirement 3: Protect Stored Account Data

Requirement Description
3.1 Processes and mechanisms for protecting stored account data are defined and understood.

PCI DSS Requirement
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 3 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.1.2.a Examine documentation to verify that descriptions of roles and responsibilities performing activities in Requirement 3 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
3.1.2.b Interview personnel with responsibility for performing activities in Requirement 3 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
3.2 Storage of account data is kept to a minimum.

PCI DSS Requirement
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a **best practice** until **31 March 2025**, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.* • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.2.1.a Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **data retention and disposal policies, procedures, and processes** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
3.2.1.b Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy.	**Identify** the evidence reference number(s) from Section 6 for all **files and system records** examined for this testing procedure.	
3.2.1.c Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.	**Identify** the evidence reference number(s) from Section 6 for the **observations of the mechanisms used** for this testing procedure.	

Requirement Description
3.3 Sensitive authentication data (SAD) is not stored after authorization.

PCI DSS Requirement
3.3.1 SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach Appendix C to support this method.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.3.1.a If SAD is received, examine documented policies, procedures, and system configurations to verify the data is not stored after authorization.	**Identify** the evidence reference number(s) from Section 6 for all **documented policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
3.3.1.b If SAD is received, examine the documented procedures and observe the secure data deletion processes to verify the data is rendered unrecoverable upon completion of the authorization process.	**Identify** the evidence reference number(s) from Section 6 for all **documented procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for the **observations of the secure data deletion processes** for this testing procedure.	

PCI DSS Requirement					
3.3.1.1 The full contents of any track are not stored upon completion of the authorization process.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach Appendix C to support this method.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
3.3.1.1 Examine data sources to verify that the full contents of any track are not stored upon completion of the authorization process.	**Identify** the evidence reference number(s) from Section 6 for all **data sources** examined for this testing procedure.				

PCI DSS Requirement					
3.3.1.2 The card verification code is not stored upon completion of the authorization process.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach Appendix C to support this method.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.3.1.2 Examine data sources, to verify that the card verification code is not stored upon completion of the authorization process.	**Identify** the evidence reference number(s) from Section 6 for all **data sources** examined for this testing procedure.	

PCI DSS Requirement					
3.3.1.3 The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach Appendix C to support this method.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.3.1.3 Examine data sources, to verify that PINs and PIN blocks are not stored upon completion of the authorization process.	**Identify** the evidence reference number(s) from Section 6 for all **data sources** examined for this testing procedure.	

PCI DSS Requirement
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach Appendix C to support this method.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.3.2 Examine data stores, system configurations, and/or vendor documentation to verify that all SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	**Identify** the evidence reference number(s) from Section 6 for all **data stores** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	

PCI DSS Requirement					
3.3.3 ***Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:*** Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. *This bullet is a* ***best practice*** *until* ***31 March 2025****, after which it will be required as part of Requirement 3.3.3 and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
3.3.3.a ***Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data:*** Examine documented policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.	Identify the evidence reference number(s) from Section 6 for all **documented policies** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
3.3.3.b ***Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data:*** Examine data stores and system configurations to verify that the sensitive authentication data is stored securely.	Identify the evidence reference number(s) from Section 6 for all **data stores** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.				

Requirement Description
3.4 Access to displays of full PAN and ability to copy PAN are restricted.

PCI DSS Requirement
3.4.1 PAN is masked when displayed (the BIN and last four digits **are the maximum number** of digits to be displayed), such that only personnel with a legitimate business need can see **more than** the BIN and last four digits of the PAN.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.4.1.a Examine documented policies and procedures for masking the display of PANs to verify: • A list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN is masked when displayed such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	**Identify** the evidence reference number(s) from Section 6 for all **documented policies and procedures** examined for this testing procedure.	
3.4.1.b Examine system configurations to verify that full PAN is only displayed for roles with a documented business need, and that PAN is masked for all other requests.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
3.4.1.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displayed, and that only those with a legitimate business need are able to see more than the BIN and/or last four digits of the PAN.	**Identify** the evidence reference number(s) from Section 6 for all **displays of PAN** examined for this testing procedure.	

PCI DSS Requirement					
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
3.4.2.a Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.	**Identify** the evidence reference number(s) from Section 6 for all **documented policies and procedures** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **documented evidence for technical controls** examined for this testing procedure.				

3.4.2.b Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	
3.4.2.c Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	**Identify** the evidence reference number(s) from Section 6 for all **observations** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description

3.5 Primary account number (PAN) is secured wherever it is stored.

PCI DSS Requirement

3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches:

- One-way hashes based on strong cryptography of the entire PAN.
- Truncation (hashing cannot be used to replace the truncated segment of PAN).
  - If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN.
- Index tokens.
- Strong cryptography with associated key-management processes and procedures.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*		
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**
3.5.1.a Examine documentation about the system used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the methods specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
3.5.1.b Examine data repositories and audit logs, including payment application logs, to verify the PAN is rendered unreadable using any of the methods specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **data repositories** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **audit logs** examined for this testing procedure.	
3.5.1.c If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	**Identify** the evidence reference number(s) from Section 6 for all **implemented controls** examined for this testing procedure.	

PCI DSS Requirement
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7. ***Note:*** *This requirement is considered a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment. This requirement will replace the bullet in Requirement 3.5.1 for one-way hashes once its effective date is reached.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.5.1.1.a Examine documentation about the hashing method used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (as applicable) to verify that the hashing method results in keyed cryptographic hashes of the entire PAN, with associated key management processes and procedures.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
3.5.1.1.b Examine documentation about the key management procedures and processes associated with the keyed cryptographic hashes to verify keys are managed in accordance with Requirements 3.6 and 3.7.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

3.5.1.1.c Examine data repositories to verify the PAN is rendered unreadable.	**Identify** the evidence reference number(s) from Section 6 for all **data repositories** examined for this testing procedure.	
3.5.1.1.d Examine audit logs, including payment application logs, to verify the PAN is rendered unreadable.	**Identify** the evidence reference number(s) from Section 6 for all **audit logs** examined for this testing procedure.	

PCI DSS Requirement
3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media OR • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1. ***Note:*** *This requirement is considered a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.5.1.2.a Examine encryption processes to verify that, if disk-level or partition-level encryption is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media, OR • If used for non-removable electronic media, examine encryption processes used to verify that PAN is also rendered unreadable via another method that meets Requirement 3.5.1.	**Identify** the evidence reference number(s) from Section 6 for all **encryption processes** examined for this testing procedure.	
3.5.1.2.b Examine configurations and/or vendor documentation and observe encryption processes to verify the system is configured according to vendor documentation the result is that the disk or the partition is rendered unreadable.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for the **observations of the encryption processes** for this testing procedure.	

PCI DSS Requirement
3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field-level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.5.1.3.a If disk-level or partition-level encryption is used to render PAN unreadable, examine the system configuration and observe the authentication process to verify that logical access is implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of the authentication process** for this testing procedure.	
3.5.1.3.b Examine files containing authentication factors (passwords, passphrases, or cryptographic keys) and interview personnel to verify that authentication factors that allow access to unencrypted data are stored securely and are independent from the native operating system's authentication and access control methods.	**Identify** the evidence reference number(s) from Section 6 for all **files containing authentication factors** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
3.6 Cryptographic keys used to protect stored account data are secured.

PCI DSS Requirement
3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.6.1 Examine documented key-management policies and procedures to verify that processes to protect cryptographic keys used to protect stored account data against disclosure and misuse are defined to include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all documentation examined for this testing procedure.	

PCI DSS Requirement
3.6.1.1 ***Additional requirement for service providers only:*** A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a* ***best practice*** *until* ***31 March 2025****, after which it will be required as part of Requirement 3.6.1 and must be fully considered during a PCI DSS assessment.* • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, to support meeting Requirement 12.3.4.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.6.1.1 ***Additional testing procedure for service provider assessments only*****:** Interview responsible personnel and examine documentation to verify that a document exists to describe the cryptographic architecture that includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement
3.6.1.2 Secret and private keys used to protect stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.6.1.2.a Examine documented procedures to verify it is defined that cryptographic keys used to encrypt/decrypt stored account data must exist only in one (or more) of the forms specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented procedures** examined for this testing procedure.	
3.6.1.2.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt stored account data exist in one (or more) of the forms specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **key storage** locations examined for this testing procedure.	

3.6.1.2.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **key storage locations** examined for this testing procedure.	

PCI DSS Requirement					
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
3.6.1.3 Examine user access lists to verify that access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	**Identify** the evidence reference number(s) from Section 6 for all **user access lists** examined for this testing procedure.				

PCI DSS Requirement					
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.6.1.4 Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	**Identify** the evidence reference number(s) from Section 6 for all **key storage locations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.	

Requirement Description
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

PCI DSS Requirement
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.7.1.a Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define generation of strong cryptographic keys.	**Identify** the evidence reference number(s) from Section 6 for all **documented key-management policies and procedures** examined for this testing procedure.	
3.7.1.b Observe the method for generating keys to verify that strong keys are generated.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the methods for generating keys** for this testing procedure.	

PCI DSS Requirement					
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
3.7.2.a Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure distribution of cryptographic keys.	**Identify** the evidence reference number(s) from Section 6 for the **documented key management policies and procedures** examined for this testing procedure.				
3.7.2.b Observe the method for distributing keys to verify that keys are distributed securely.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the method for distributing keys** for this testing procedure.				

PCI DSS Requirement					
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.7.3.a Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure storage of cryptographic keys.	**Identify** the evidence reference number(s) from Section 6 for the **documented key-management policies and procedures** examined for this testing procedure.	
3.7.3.b Observe the method for storing keys to verify that keys are stored securely.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the method for storing keys** for this testing procedure.	

PCI DSS Requirement					
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**		**Reporting Details: Assessor's Response**		
3.7.4.a Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define changes to cryptographic keys that have reached the end of their cryptoperiod and include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented key-management policies and procedures** examined for this testing procedure.				
3.7.4.b Interview personnel, examine documentation, and observe key storage locations to verify that keys are changed at the end of the defined cryptoperiod(s). *(continued)*	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				

3.7.4.b *(cont.)*	**Identify** the evidence reference number(s) from Section 6 for all **observations of key storage locations** for this testing procedure.	

PCI DSS Requirement
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. • Retired or replaced keys are not used for encryption operations.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.7.5.a Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define retirement, replacement, or destruction of keys in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented key-management policies and procedures** examined for this testing procedure.	
3.7.5.b Interview personnel to verify that processes are implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented, including managing these operations using split knowledge and dual control.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
3.7.6.a Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define using split knowledge and dual control.	**Identify** the evidence reference number(s) from Section 6 for all **documented key-management policies and procedures** examined for this testing procedure.				
3.7.6.b Interview personnel and/or observe processes to verify that manual cleartext keys are managed with split knowledge and dual control.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.				

PCI DSS Requirement					
3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.7.7.a Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define prevention of unauthorized substitution of cryptographic keys.	**Identify** the evidence reference number(s) from Section 6 for the **documented key-management policies and procedures** examined for this testing procedure.	
3.7.7.b Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.	

PCI DSS Requirement					
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.7.8.a Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define acknowledgments for key custodians in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented key-management policies and procedures** examined for this testing procedure.	
3.7.8.b Examine documentation or other evidence showing that key custodians have provided acknowledgments in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation or other evidence** examined for this testing procedure.	

PCI DSS Requirement					
3.7.9 ***Additional requirement for service providers only:*** Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
3.7.9 ***Additional testing procedure for service provider assessments only:*** If the service provider shares cryptographic keys with its customers for transmission or storage of account data, examine the documentation that the service provider provides to its customers to verify it includes guidance on how to securely transmit, store, and update customers' keys in accordance with all elements specified in Requirements 3.7.1 through 3.7.8 above.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Requirement Description
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.

PCI DSS Requirement
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
4.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 4 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
4.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 4 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
4.1.2.b Interview personnel with responsibility for performing activities in Requirement 4 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

Requirement Description
4.2 PAN is protected with strong cryptography during transmission.

PCI DSS Requirement
4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a* **best practice** *until* ***31 March 2025****, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.* • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
4.2.1.a Examine documented policies and procedures and interview personnel to verify processes are defined to include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

4.2.1.b Examine system configurations to verify that strong cryptography and security protocols are implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
4.2.1.c Examine cardholder data transmissions to verify that all PAN is encrypted with strong cryptography when it is transmitted over open, public networks.	**Identify** the evidence reference number(s) from Section 6 for all **cardholder data transmissions** examined for this testing procedure.	
4.2.1.d Examine system configurations to verify that keys and/or certificates that cannot be verified as trusted are rejected.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

PCI DSS Requirement					
4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
4.2.1.1.a Examine documented policies and procedures to verify processes are defined for the entity to maintain an inventory of its trusted keys and certificates.	**Identify** the evidence reference number(s) from Section 6 for the **documented policies and procedures** examined for this testing procedure.	
4.2.1.1.b Examine the inventory of trusted keys and certificates to verify it is kept up to date.	**Identify** the evidence reference number(s) from Section 6 for all **inventories of trusted keys** examined for this testing procedure.	

PCI DSS Requirement
4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
4.2.1.2 Examine system configurations to verify that wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

PCI DSS Requirement					
4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
4.2.2.a Examine documented policies and procedures to verify that processes are defined to secure PAN with strong cryptography whenever sent over end-user messaging technologies.	**Identify** the evidence reference number(s) from Section 6 for all **documented policies and procedures** examined for this testing procedure.	
4.2.2.b Examine system configurations and vendor documentation to verify that PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software

Requirement Description
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

PCI DSS Requirement
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
5.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 5 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
5.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 5 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
5.1.2.b Interview personnel with responsibility for performing activities in Requirement 5 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

Requirement Description
5.2 Malicious software (malware) is prevented or detected and addressed.

PCI DSS Requirement
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
5.2.1.a Examine system components to verify that an anti-malware solution(s) is deployed on all system components, except for those determined to not be at risk from malware based on periodic evaluations per Requirement 5.2.3.	**Identify** the evidence reference number(s) from Section 6 for all **system components** examined for this testing procedure.	
5.2.1.b For any system components without an anti-malware solution, examine the periodic evaluations to verify the component was evaluated and the evaluation concludes that the component is not at risk from malware.	**Identify** the evidence reference number(s) from Section 6 for all **periodic evaluations** examined for this testing procedure.	

PCI DSS Requirement					
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**		**Reporting Details: Assessor's Response**		
5.2.2 Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.				

PCI DSS Requirement					
5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
5.2.3.a Examine documented policies and procedures to verify that a process is defined for periodic evaluations of any system components that are not at risk for malware that includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented policies and procedures** examined for this testing procedure.				
5.2.3.b Interview personnel to verify that the evaluations include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

5.2.3.c Examine the list of system components identified as not at risk of malware and compare to the system components without an anti-malware solution deployed per Requirement 5.2.1 to verify that the system components match for both requirements.	**Identify** the evidence reference number(s) from Section 6 for all **lists of system components** examined for this testing procedure.	

PCI DSS Requirement					
5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
5.2.3.1.a Examine the entity's targeted risk analysis for the frequency of periodic evaluations of system components identified as not at risk for malware to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	**Identify** the evidence reference number(s) from Section 6 for the **targeted risk analysis** examined for this testing procedure.				
5.2.3.1.b Examine documented results of periodic evaluations of system components identified as not at risk for malware and interview personnel to verify that evaluations are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented results of periodic evaluations of system components** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

Requirement Description
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

PCI DSS Requirement
5.3.1 The anti-malware solution(s) is kept current via automatic updates.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
5.3.1.a Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution is configured to perform automatic updates.	**Identify** the evidence reference number(s) from Section 6 for all **anti-malware solution(s) configurations** examined for this testing procedure.	
5.3.1.b Examine system components and logs, to verify that the anti-malware solution(s) and definitions are current and have been promptly deployed	**Identify** the evidence reference number(s) from Section 6 for all **system components** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **logs** examined for this testing procedure.	

PCI DSS Requirement
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
5.3.2.a Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution(s) is configured to perform at least one of the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **anti-malware solution(s) configurations** examined for this testing procedure.	
5.3.2.b Examine system components, including all operating system types identified as at risk for malware, to verify the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system components** examined for this testing procedure.	

5.3.2.c Examine logs and scan results to verify that the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **logs** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **scan results** examined for this testing procedure.	

PCI DSS Requirement					
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**		**Reporting Details: Assessor's Response**		
5.3.2.1.a Examine the entity's targeted risk analysis for the frequency of periodic malware scans to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	**Identify** the evidence reference number(s) from Section 6 for the **targeted risk analysis** examined for this testing procedure.				
5.3.2.1.b Examine documented results of periodic malware scans and interview personnel to verify scans are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented results of periodic malware scans** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement
5.3.3 For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
5.3.3.a Examine anti-malware solution(s) configurations to verify that, for removable electronic media, the solution is configured to perform at least one of the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **anti-malware solution(s) configurations** examined for this testing procedure.	
5.3.3.b Examine system components with removable electronic media connected to verify that the solution(s) is enabled in accordance with at least one of the elements as specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system components** examined for this testing procedure.	

5.3.3.c Examine logs and scan results to verify that the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **logs** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **scan results** examined for this testing procedure.	

PCI DSS Requirement
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
5.3.4 Examine anti-malware solution(s) configurations to verify logs are enabled and retained in accordance with Requirement 10.5.1.	**Identify** the evidence reference number(s) from Section 6 for all **anti-malware solution(s) configurations** examined for this testing procedure.	

PCI DSS Requirement
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
5.3.5.a Examine anti-malware configurations, to verify that the anti-malware mechanisms cannot be disabled or altered by users.	**Identify** the evidence reference number(s) from Section 6 for all **anti-malware solution configurations** examined for this testing procedure.	
5.3.5.b Interview responsible personnel and observe processes to verify that any requests to disable or alter anti-malware mechanisms are specifically documented and authorized by management on a case-by-case basis for a limited time period.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.	

Requirement Description
5.4 Anti-phishing mechanisms protect users against phishing attacks.

PCI DSS Requirement
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
5.4.1 Observe implemented processes and examine mechanisms to verify controls are in place to detect and protect personnel against phishing attacks.	**Identify** the evidence reference number(s) from Section 6 for all **observations of implemented processes** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **mechanisms** examined for this testing procedure.	

Requirement 6: Develop and Maintain Secure Systems and Software

Requirement Description
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

PCI DSS Requirement
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 6 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 6 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
6.1.2.b Interview personnel responsible for performing activities in Requirement 6 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
6.2 Bespoke and custom software are developed securely.

PCI DSS Requirement
6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.2.1 Examine documented software development procedures to verify that processes are defined that include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented software development procedures** examined for this testing procedure.	

PCI DSS Requirement
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.2.2.a Examine software development procedures to verify that processes are defined for training of software development personnel developing bespoke and custom software that includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **software development procedures** examined for this testing procedure.	
6.2.2.b Examine training records and interview personnel to verify that software development personnel working on bespoke and custom software received software security training that is relevant to their job function and development languages in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **training records** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.2.3.a Examine documented software development procedures and interview responsible personnel to verify that processes are defined that require all bespoke and custom software to be reviewed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented software development procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
6.2.3.b Examine evidence of changes to bespoke and custom software to verify that the code changes were reviewed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **evidence of changes** examined for this testing procedure.	

PCI DSS Requirement					
6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. • Reviewed and approved by management prior to release.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
6.2.3.1.a If manual code reviews are performed for bespoke and custom software prior to release to production, examine documented software development procedures and interview responsible personnel to verify that processes are defined for manual code reviews to be conducted in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented software development procedures** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
6.2.3.1.b Examine evidence of changes to bespoke and custom software and interview personnel to verify that manual code reviews were conducted in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **evidence of changes** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement
6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.2.4 Examine documented procedures and interview responsible software development personnel to verify that software engineering techniques or other methods are defined and in use by developers of bespoke and custom software to prevent or mitigate all common software attacks as specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
6.3 Security vulnerabilities are identified and addressed.

PCI DSS Requirement
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.3.1.a Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	

6.3.1.b Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.	

PCI DSS Requirement					
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
6.3.2.a Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
6.3.2.b Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.	**Identify** the evidence reference number(s) from Section 6 for all **software documentation** examined for this testing procedure.				

PCI DSS Requirement
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment as identified according to the risk ranking process at Requirement 6.3.1.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.3.3.a Examine policies and procedures to verify processes are defined for addressing vulnerabilities by installing applicable security patches/updates in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
6.3.3.b Examine system components and related software and compare the list of installed security patches/updates to the most recent security patch/update information to verify vulnerabilities are addressed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system components and related software** examined for this testing procedure.	

Requirement Description
6.4 Public-facing web applications are protected against attacks.

PCI DSS Requirement
6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web-based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated. ***Note:*** *This requirement will be* ***superseded*** *by Requirement 6.4.2 after* ***31 March 2025*** *when Requirement 6.4.2 becomes effective.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.4.1 For public-facing web applications, ensure that either one of the required methods is in place as follows: • If manual or automated vulnerability security assessment tools or methods are in use, examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed in accordance with all elements of this requirement specific to the tool/method. OR • If an automated technical solution(s) is installed that continually detects and prevents web-based attacks, examine the system configuration settings and audit logs, and interview responsible personnel to verify that the automated technical solution(s) is installed in accordance with all elements of this requirement specific to the solution(s).	**Identify** the evidence reference number(s) from Section 6 for all **documented processes** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **records of application security assessments** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **audit logs** examined for this testing procedure.	

PCI DSS Requirement
6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment. This new requirement will replace Requirement 6.4.1 once its effective date is reached.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.4.2 For public-facing web applications, examine the system configuration settings and audit logs, and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks is in place in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **audit logs** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written business or technical justification as to why each is necessary. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.4.3.a Examine policies and procedures to verify that processes are defined for managing all payment page scripts that are loaded and executed in the consumer's browser, in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	

6.4.3.b Interview responsible personnel and examine inventory records and system configurations to verify that all payment page scripts that are loaded and executed in the consumer's browser are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **inventory records** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

Requirement Description
6.5 Changes to all system components are managed securely.

PCI DSS Requirement
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.5.1.a Examine documented change control procedures to verify procedures are defined for changes to all system components in the production environment to include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented change control procedures** examined for this testing procedure.	

6.5.1.b Examine recent changes to system components and trace those changes back to related change control documentation. For each change examined, verify the change is implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **recent changes to system components** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **change control documentation** examined for this testing procedure.	

PCI DSS Requirement
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.5.2 Examine documentation for significant changes, interview personnel, and observe the affected systems/networks to verify that the entity confirmed applicable PCI DSS requirements were in place on all new or changed systems and networks and that documentation was updated as applicable.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of the affected systems/networks** for this testing procedure.	

PCI DSS Requirement					
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.5.3.a Examine policies and procedures to verify that processes are defined for separating the pre-production environment from the production environment via access controls that enforce the separation.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
6.5.3.b Examine network documentation and configurations of network security controls to verify that the pre-production environment is separate from the production environment(s).	**Identify** the evidence reference number(s) from Section 6 for all **network documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	
6.5.3.c Examine access control settings to verify that access controls are in place to enforce separation between the pre-production and production environment(s).	**Identify** the evidence reference number(s) from Section 6 for all **access control settings** examined for this testing procedure.	

PCI DSS Requirement					
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
6.5.4.a Examine policies and procedures to verify that processes are defined for separating roles and functions to provide accountability such that only reviewed and approved changes are deployed.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.				
6.5.4.b Observe processes and interview personnel to verify implemented controls separate roles and functions and provide accountability such that only reviewed and approved changes are deployed.	**Identify** the evidence reference number(s) from Section 6 for all **observations of processe**s for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
6.5.5.a Examine policies and procedures to verify that processes are defined for not using live PANs in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.				
6.5.5.b Observe testing processes and interview personnel to verify procedures are in place to ensure live PANs are not used in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the testing processes** for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

6.5.5.c Examine pre-production test data to verify live PANs are not used in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	**Identify** the evidence reference number(s) from Section 6 for all **pre-production test data** examined for this testing procedure.	

PCI DSS Requirement					
6.5.6 Test data and test accounts are removed from system components before the system goes into production.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
6.5.6.a Examine policies and procedures to verify that processes are defined for removal of test data and test accounts from system components before the system goes into production.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
6.5.6.b Observe testing processes for both off-the-shelf software and in-house applications, and interview personnel to verify test data and test accounts are removed before a system goes into production.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the testing processes** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
6.5.6.c Examine data and accounts for recently installed or updated off-the-shelf software and in-house applications to verify there is no test data or test accounts on systems in production.	**Identify** the evidence reference number(s) from Section 6 for all **data** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **accounts** examined for this testing procedure.	

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

Requirement Description
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

PCI DSS Requirement
7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
7.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 7 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
7.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 7 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
7.1.2.b Interview personnel with responsibility for performing activities in Requirement 7 to verify that roles and responsibilities are assigned as and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

Requirement Description
7.2 Access to system components and data is appropriately defined and assigned.

PCI DSS Requirement
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
7.2.1.a Examine documented policies and procedures and interview personnel to verify the access control model is defined in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
7.2.1.b Examine access control model settings and verify that access needs are appropriately defined in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **access control model settings** examined for this testing procedure.	

PCI DSS Requirement					
7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
7.2.2.a Examine policies and procedures to verify they cover assigning access to users in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
7.2.2.b Examine user access settings, including for privileged users, and interview responsible management personnel to verify that privileges assigned are in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **user access settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
7.2.2.c Interview personnel responsible for assigning access to verify that privileged user access is assigned in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
7.2.3 Required privileges are approved by authorized personnel.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
7.2.3.a Examine policies and procedures to verify they define processes for approval of all privileges by authorized personnel.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
7.2.3.b Examine user IDs and assigned privileges, and compare with documented approvals to verify that: • Documented approval exists for the assigned privileges. • The approval was by authorized personnel. • Specified privileges match the roles assigned to the individual.	**Identify** the evidence reference number(s) from Section 6 for all **user IDs and assigned privileges** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documented approvals** examined for this testing procedure.	

PCI DSS Requirement
7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
7.2.4.a Examine policies and procedures to verify they define processes to review all user accounts and related access privileges, including third-party/vendor accounts, in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	

7.2.4.b Interview responsible personnel and examine documented results of periodic reviews of user accounts to verify that all the results are in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for the **documented results of periodic reviews of user accounts** examined for this testing procedure.	

PCI DSS Requirement					
7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
7.2.5.a Examine policies and procedures to verify they define processes to manage and assign application and system accounts and related access privileges in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.				
7.2.5.b Examine privileges associated with system and application accounts and interview responsible personnel to verify that application and system accounts and related access privileges are assigned and managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **privileges associated with system and application accounts** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement
7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
7.2.5.1.a Examine policies and procedures to verify they define processes to review all application and system accounts and related access privileges in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
7.2.5.1.b Examine the entity's targeted risk analysis for the frequency of periodic reviews of application and system accounts and related access privileges to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	**Identify** the evidence reference number(s) from Section 6 for the **entity's targeted risk analysis** examined for this testing procedure.	

7.2.5.1.c Interview responsible personnel and examine documented results of periodic reviews of system and application accounts and related privileges to verify that the reviews occur in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documented results of periodic reviews** examined for this testing procedure.	

PCI DSS Requirement					
7.2.6 All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
7.2.6.a Examine policies and procedures and interview personnel to verify processes are defined for granting user access to query repositories of stored cardholder data, in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
7.2.6.b Examine configuration settings for querying repositories of stored cardholder data to verify they are in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.				

Requirement Description
7.3 Access to system components and data is managed via an access control system(s).

PCI DSS Requirement
7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
7.3.1 Examine vendor documentation and system settings to verify that access is managed for each system component via an access control system(s) that restricts access based on a user's need to know and covers all system components.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system settings** examined for this testing procedure.	

PCI DSS Requirement					
7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
7.3.2 Examine vendor documentation and system settings to verify that the access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **system settings** examined for this testing procedure.				

PCI DSS Requirement					
7.3.3 The access control system(s) is set to “deny all” by default.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the “Required Reporting” column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor’s Response			
7.3.3 Examine vendor documentation and system settings to verify that the access control system(s) is set to “deny all” by default.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **system settings** examined for this testing procedure.				

Requirement 8: Identify Users and Authenticate Access to System Components

Requirement Description
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

PCI DSS Requirement
8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures that are identified in Requirement 8 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 8 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
8.1.2.b Interview personnel with responsibility for performing activities in Requirement 8 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

PCI DSS Requirement
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.2.1.a Interview responsible personnel to verify that all users are assigned a unique ID for access to system components and cardholder data.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
8.2.1.b Examine audit logs and other evidence to verify that access to system components and cardholder data can be uniquely identified and associated with individuals.	**Identify** the evidence reference number(s) from Section 6 for all **audit logs** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for **any other evidence** examined for this testing procedure.	

PCI DSS Requirement
8.2.2 Group, shared, or generic IDs, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • ID use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.2.2.a Examine user account lists on system components and applicable documentation to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **user account lists** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

8.2.2.b Examine authentication policies and procedures to verify processes are defined for shared authentication credentials such that they are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **authentication policies and procedures** examined for this testing procedure.	
8.2.2.c Interview system administrators to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
8.2.3 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises use unique authentication factors for each customer premises.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.2.3 ***Additional testing procedure for service provider assessments only:*** Examine authentication policies and procedures and interview personnel to verify that service providers with remote access to customer premises use unique authentication factors for remote access to each customer premises.	**Identify** the evidence reference number(s) from Section 6 for all **authentication policies and procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
8.2.4 Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions) and examine system settings to verify the activity has been managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented authorizations** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **system settings** examined for this testing procedure.				

PCI DSS Requirement					
8.2.5 Access for terminated users is immediately revoked.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.2.5.a Examine information sources for terminated users and review current user access lists—for both local and remote access—to verify that terminated user IDs have been deactivated or removed from the access lists.	**Identify** the evidence reference number(s) from Section 6 for all **information sources** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **current user access lists** examined for this testing procedure.	
8.2.5.b Interview responsible personnel to verify that all physical authentication factors—such as, smart cards, tokens, etc.—have been returned or deactivated for terminated users.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.2.6 Examine user accounts and last logon information, and interview personnel to verify that any inactive user accounts are removed or disabled within 90 days of inactivity.	**Identify** the evidence reference number(s) from Section 6 for all **user accounts and last login information** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
8.2.7 Interview personnel, examine documentation for managing accounts, and examine evidence to verify that accounts used by third parties for remote access are managed according to all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for any **other evidence** examined for this testing procedure.				

PCI DSS Requirement					
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
8.2.8 Examine system configuration settings to verify that system/session idle timeout features for user sessions have been set to 15 minutes or less.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.				

Requirement Description
8.3 Strong authentication for users and administrators is established and managed.

PCI DSS Requirement
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • 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 element.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.1.a Examine documentation describing the authentication factor(s) used to verify that user access to system components is authenticated via at least one authentication factor specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
8.3.1.b For each type of authentication factor used with each type of system component, observe an authentication to verify that authentication is functioning consistently with documented authentication factor(s).	**Identify** the evidence reference number(s) from Section 6 for all **observations of each type of authentication factor used** for this testing procedure.	

PCI DSS Requirement					
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.2.a Examine vendor documentation and system configuration settings to verify that authentication factors are rendered unreadable with strong cryptography during transmission and storage.	**Identify** the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	
8.3.2.b Examine repositories of authentication factors to verify that they are unreadable during storage.	**Identify** the evidence reference number(s) from Section 6 for all **repositories of authentication factors** examined for this testing procedure.	
8.3.2.c Examine data transmissions to verify that authentication factors are unreadable during transmission.	**Identify** the evidence reference number(s) from Section 6 for all **data transmissions** examined for this testing procedure.	

PCI DSS Requirement					
8.3.3 User identity is verified before modifying any authentication factor.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.3 Examine procedures for modifying authentication factors and observe security personnel to verify that when a user requests a modification of an authentication factor, the user's identity is verified before the authentication factor is modified.	**Identify** the evidence reference number(s) from Section 6 for all **procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of security personnel** for this testing procedure.	

PCI DSS Requirement
8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.4.a Examine system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than 10 invalid logon attempts.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	
8.3.4.b Examine 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 the user's identity is confirmed.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

PCI DSS Requirement					
8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**		**Reporting Details: Assessor's Response**		
8.3.5 Examine procedures for setting and resetting passwords/passphrases (if used as authentication factors to meet Requirement 8.3.1) and observe security personnel to verify that passwords/passphrases are set and reset in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **procedures** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **observations of security personnel** for this testing procedure.				

PCI DSS Requirement
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment. Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.6 Examine system configuration settings to verify that user password/passphrase complexity parameters are set in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

PCI DSS Requirement					
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.7 Examine system configuration settings to verify that password parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

PCI DSS Requirement
8.3.8 Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.8.a Examine procedures and interview personnel to verify that authentication policies and procedures are distributed to all users.	**Identify** the evidence reference number(s) from Section 6 for all **procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
8.3.8.b Review authentication policies and procedures that are distributed to users and verify they include the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **authentication policies and procedures** examined for this testing procedure.	

8.3.8.c Interview users to verify that they are familiar with authentication policies and procedures.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.9 If passwords/passphrases are used as the only authentication factor for user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

PCI DSS Requirement
8.3.10 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed. ***Note****: This requirement for service providers will be* ***superseded*** *by Requirement 8.3.10.1 once 8.3.10.1 becomes effective.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.10 ***Additional testing procedure for service provider assessments only:*** If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data, examine guidance provided to customer users to verify that the guidance includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **guidance provided to customer users** examined for this testing procedure.	

PCI DSS Requirement
8.3.10.1 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment. Until this requirement is effective on 31 March 2025, service providers may meet either Requirement 8.3.10 or 8.3.10.1.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.3.10.1 ***Additional testing procedure for service provider assessments only:*** If passwords/passphrases are used as the only authentication factor for customer user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

PCI DSS Requirement					
8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
8.3.11.a Examine authentication policies and procedures to verify that procedures for using authentication factors such as physical security tokens, smart cards, and certificates are defined and include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **authentication policies and procedures** examined for this testing procedure.				
8.3.11.b Interview security personnel to verify authentication factors are assigned to an individual user and not shared among multiple users.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

8.3.11.c Examine system configuration settings and/or observe physical controls, as applicable, to verify that controls are implemented to ensure only the intended user can use that factor to gain access.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of physical controls** conducted for this testing procedure.	

Requirement Description
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.

PCI DSS Requirement
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.4.1.a Examine network and/or system configurations to verify MFA is required for all non-console into the CDE for personnel with administrative access.	**Identify** the evidence reference number(s) from Section 6 for all **network and/or system configurations** examined for this testing procedure.	
8.4.1.b Observe administrator personnel logging into the CDE and verify that MFA is required.	**Identify** the evidence reference number(s) from Section 6 for all **observations of administrator personnel logging into the CDE** for this testing procedure.	

PCI DSS Requirement					
8.4.2 MFA is implemented for all non-console access into the CDE. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
8.4.2.a Examine network and/or system configurations to verify MFA is implemented for all non-console access into the CDE.	**Identify** the evidence reference number(s) from Section 6 for all **network and/or system configurations** examined for this testing procedure.				
8.4.2.b Observe personnel logging in to the CDE and examine evidence to verify that MFA is required.	**Identify** the evidence reference number(s) from Section 6 for all **observations of personnel logging into the CDE** for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for any **additional evidence** examined for this testing procedure.				

PCI DSS Requirement
8.4.3 MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.4.3.a Examine network and/or system configurations for remote access servers and systems to verify MFA is required in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **network and/or system configurations** examined for this testing procedure.	
8.4.3.b Observe personnel (for example, users and administrators) and third parties connecting remotely to the network and verify that multi-factor authentication is required.	**Identify** the evidence reference number(s) from Section 6 for all **observations of personnel connecting remotely to the network** for this testing procedure.	

Requirement Description
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

PCI DSS Requirement
8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected.

Note*: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*

**As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.5.1.a Examine vendor system documentation to verify that the MFA system is not susceptible to replay attacks.	**Identify** the evidence reference number(s) from Section 6 for all **vendor system documentation** examined for this testing procedure.	
8.5.1.b Examine system configurations for the MFA implementation to verify it is configured in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

8.5.1.c Interview responsible personnel and observe processes to verify that any requests to bypass MFA are specifically documented and authorized by management on an exception basis, for a limited time period.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.	
8.5.1.d Observe personnel logging into system components in the CDE to verify that access is granted only after all authentication factors are successful.	**Identify** the evidence reference number(s) from Section 6 for all **observations of personnel logging into system components in the CDE** for this testing procedure.	
8.5.1.e Observe personnel connecting remotely from outside the entity's network to verify that access is granted only after all authentication factors are successful.	**Identify** the evidence reference number(s) from Section 6 for all **observations of personnel connecting remotely from outside the entity's network** for this testing procedure.	

Requirement Description
8.6 Use of application and system accounts and associated authentication factors is strictly managed.

PCI DSS Requirement
8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.6.1 Examine application and system accounts that can be used interactively and interview administrative personnel to verify that application and system accounts are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **application and system accounts** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
8.6.2.a Interview personnel and examine system development procedures to verify that processes are defined for application and system accounts that can be used for interactive login, specifying that passwords/passphrases are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **system development procedures** examined for this testing procedure.				
8.6.2.b Examine scripts, configuration/property files, and bespoke and custom source code for application and system accounts that can be used for interactive login, to verify passwords/passphrases for those accounts are not present.	**Identify** the evidence reference number(s) from Section 6 for all **scripts, configuration/property files, and bespoke and custom source code** examined for this testing procedure.				

PCI DSS Requirement
8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
8.6.3.a Examine policies and procedures to verify that procedures are defined to protect passwords/passphrases for application or system accounts against misuse in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	

8.6.3.b Examine the entity's targeted risk analysis for the change frequency and complexity for passwords/passphrases for application and system accounts to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1 and addresses: • The frequency defined for periodic changes to application and system passwords/passphrases. • The complexity defined for passwords/passphrases and appropriateness of the complexity relative to the frequency of changes.	**Identify** the evidence reference number(s) from Section 6 for the **entity's targeted risk analysis** examined for this testing procedure.	
8.6.3.c Interview responsible personnel and examine system configuration settings to verify that passwords/passphrases for any application and system accounts are protected against misuse in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

Requirement 9: Restrict Physical Access to Cardholder Data

Requirement Description
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

PCI DSS Requirement
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 9 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 9 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
9.1.2.b Interview personnel with responsibility for performing activities in Requirement 9 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

PCI DSS Requirement
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.2.1 Observe entry controls and interview responsible personnel to verify that physical security controls are in place to restrict access to systems in the CDE.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the entry controls** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.2.1.1.a Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are in place to monitor the entry and exit points.	**Identify** the evidence reference number(s) from Section 6 for all **observations of locations where individual physical access to sensitive areas within the CDE occurs** for this testing procedure.	
9.2.1.1.b Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are protected from tampering or disabling.	**Identify** the evidence reference number(s) from Section 6 for all **observations of locations where individual physical access to the CDE occurs** for this testing procedure.	

9.2.1.1.c Observe the physical access control mechanisms and/or examine video cameras and interview responsible personnel to verify that: • Collected data from video cameras and/or physical access control mechanisms is reviewed and correlated with other entries. • Collected data is stored for at least three months.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the physical access control mechanisms** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **video cameras** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.2.2 Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks within the facility.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of the locations of publicly accessible network jacks** for this testing procedure.	

PCI DSS Requirement
9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.2.3 Interview responsible personnel and observe locations of hardware and lines to verify that physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of the locations of hardware and lines** for this testing procedure.	

PCI DSS Requirement					
9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.2.4 Observe a system administrator's attempt to log into consoles in sensitive areas and verify that they are "locked" to prevent unauthorized use.	**Identify** the evidence reference number(s) from Section 6 for **all observations of a system administrator's attempt to log into consoles in sensitive areas** for this testing procedure.	

Requirement Description
9.3 Physical access for personnel and visitors is authorized and managed.

PCI DSS Requirement
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.3.1.a Examine documented procedures to verify that procedures to authorize and manage physical access of personnel to the CDE are defined in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
9.3.1.b Observe identification methods, such as ID badges, and processes to verify that personnel in the CDE are clearly identified.	**Identify** the evidence reference number(s) from Section 6 for all **observations of all identification methods and processes** for this testing procedure.	

9.3.1.c Observe processes to verify that access to the identification process, such as a badge system, is limited to authorized personnel.	**Identify** the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.	

PCI DSS Requirement
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.3.1.1.a Observe personnel in sensitive areas within the CDE, interview responsible personnel, and examine physical access control lists to verify that: • Access to the sensitive area is authorized. • Access is required for the individual's job function.	**Identify** the evidence reference number(s) from Section 6 for all **observations of personnel in sensitive areas** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **physical access control lists** examined for this testing procedure.	
9.3.1.1.b Observe processes and interview personnel to verify that access of all personnel is revoked immediately upon termination.	**Identify** the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
9.3.1.1.c For terminated personnel, examine physical access controls lists and interview responsible personnel to verify that all physical access mechanisms (such as keys, access cards, etc.) were returned or disabled.	**Identify** the evidence reference number(s) from Section 6 for all **physical access control lists** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.3.2.a Examine documented procedures and interview personnel to verify procedures are defined for authorizing and managing visitor access to the CDE in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

9.3.2.b Observe processes when visitors are present in the CDE and interview personnel to verify that visitors are: • Authorized before entering the CDE. • Escorted at all times within the CDE.	**Identify** the evidence reference number(s) from Section 6 for all **observations of processes when visitors are present in the CDE** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
9.3.2.c Observe the use of visitor badges or other identification to verify that the badge or other identification does not permit unescorted access to the CDE.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the use of visitor badges or other identification** for this testing procedure.	
9.3.2.d Observe visitors in the CDE to verify that: • Visitor badges or other identification are being used for all visitors. • Visitor badges or identification easily distinguish visitors from personnel.	**Identify** the evidence reference number(s) from Section 6 for all **observations** conducted for this testing procedure.	
9.3.2.e Examine visitor badges or other identification and observe evidence in the badging system to verify visitor badges or other identification expires.	**Identify** the evidence reference number(s) from Section 6 for all **visitor badges or other identification** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of evidence in the badging system** for this testing procedure.	

PCI DSS Requirement					
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.3.3 Observe visitors leaving the facility and interview personnel to verify visitor badges or other identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. upon departure or expiration.	**Identify** the evidence reference number(s) from Section 6 for all **observations of visitors leaving the facility** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
9.3.4 Visitor logs are used to maintain a physical record of visitor activity both within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.3.4.a Examine the visitor logs and interview responsible personnel to verify that visitor logs are used to record physical access to both the facility and sensitive areas.	**Identify** the evidence reference number(s) from Section 6 for all **visitor logs** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
9.3.4.b Examine the visitor logs and verify that the logs contain: • The visitor's name and the organization represented. • The personnel authorizing physical access. • Date and time of visit.	**Identify** the evidence reference number(s) from Section 6 for all **visitor logs** examined for this testing procedure.	

9.3.4.c Examine visitor log storage locations and interview responsible personnel to verify that the log is retained for at least three months, unless otherwise restricted by law.	**Identify** the evidence reference number(s) from Section 6 for all **visitor log storage locations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

PCI DSS Requirement
9.4.1 All media with cardholder data is physically secured.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.4.1 Examine documentation to verify that procedures defined for protecting cardholder data include controls for physically securing all media.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement					
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
9.4.1.1.a Examine documentation to verify that procedures are defined for physically securing offline media backups with cardholder data in a secure location.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
9.4.1.1.b Examine logs or other documentation and interview responsible personnel at the storage location to verify that offline media backups are stored in a secure location.	**Identify** the evidence reference number(s) from Section 6 for all **logs or other documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.4.1.2.a Examine documentation to verify that procedures are defined for reviewing the security of the offline media backup location(s) with cardholder data at least once every 12 months.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
9.4.1.2.b Examine documented procedures, logs, or other documentation, and interview responsible personnel at the storage location(s) to verify that the storage location's security is reviewed at least once every 12 months.	**Identify** the evidence reference number(s) from Section 6 for all **documented procedures, logs, or other documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
9.4.2.a Examine documentation to verify that procedures are defined for classifying media with cardholder data in accordance with the sensitivity of the data.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
9.4.2.b Examine media logs or other documentation to verify that all media is classified in accordance with the sensitivity of the data.	**Identify** the evidence reference number(s) from Section 6 for all **media logs or other documentation** examined for this testing procedure.				

PCI DSS Requirement
9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.4.3.a Examine documentation to verify that procedures are defined for securing media sent outside the facility in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
9.4.3.b Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **records examined** for this testing procedure.	
9.4.3.c Examine offsite tracking logs for all media to verify tracking details are documented.	**Identify** the evidence reference number(s) from Section 6 for all **offsite tracking logs** examined for this testing procedure.	

PCI DSS Requirement					
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
9.4.4.a Examine documentation to verify that procedures are defined to ensure that media moved outside the facility is approved by management.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
9.4.4.b Examine offsite media tracking logs and interview responsible personnel to verify that proper management authorization is obtained for all media moved outside the facility (including media distributed to individuals).	**Identify** the evidence reference number(s) from Section 6 for all **offsite media tracking logs** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
9.4.5 Inventory logs of all electronic media with cardholder data are maintained.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.4.5.a Examine documentation to verify that procedures are defined to maintain electronic media inventory logs.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
9.4.5.b Examine electronic media inventory logs and interview responsible personnel to verify that logs are maintained.	**Identify** the evidence reference number(s) from Section 6 for all **electronic media inventory logs** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.4.5.1.a Examine documentation to verify that procedures are defined to conduct inventories of electronic media with cardholder data at least once every 12 months.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
9.4.5.1.b Examine electronic media inventory logs and interview personnel to verify that electronic media inventories are performed at least once every 12 months.	**Identify** the evidence reference number(s) from Section 6 for all **electronic media inventory logs** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
9.4.6.a Examine the media destruction policy to verify that procedures are defined to destroy hard-copy media with cardholder data when no longer needed for business or legal reasons in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **periodic media destruction policy examined** for this testing procedure.				
9.4.6.b Observe processes and interview personnel to verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that cardholder data cannot be reconstructed.	**Identify** the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

9.4.6.c Observe storage containers used for materials that contain information to be destroyed to verify that the containers are secure.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the storage containers used for materials that contain information to be destroyed** for this testing procedure.	

PCI DSS Requirement					
9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**		**Reporting Details: Assessor's Response**		
9.4.7.a Examine the media destruction policy to verify that procedures are defined to destroy electronic media when no longer needed for business or legal reasons in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **periodic media destruction policy examined** for this testing procedure.				
9.4.7.b Observe the media destruction process and interview responsible personnel to verify that electronic media with cardholder data is destroyed via one of the methods specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the media destruction process** for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

Requirement Description
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.

PCI DSS Requirement
9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.5.1 Examine documented policies and procedures to verify that processes are defined that include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for **policies and procedures** examined for this testing procedure.	

PCI DSS Requirement					
9.5.1.1 An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
9.5.1.1.a Examine the list of POI devices to verify it includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **lists of POI devices examined** for this testing procedure.				
9.5.1.1.b Observe POI devices and device locations and compare to devices in the list to verify that the list is accurate and up to date.	**Identify** the evidence reference number(s) from Section 6 for all **observations of the POI devices and device locations** for this testing procedure.				
9.5.1.1.c Interview personnel to verify the list of POI devices is updated when devices are added, relocated, decommissioned, etc.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.5.1.2.a Examine documented procedures to verify processes are defined for periodic inspections of POI device surfaces to detect tampering and unauthorized substitution.	**Identify** the evidence reference number(s) from Section 6 for all **documented procedures** examined for this testing procedure.	
9.5.1.2.b Interview responsible personnel and observe inspection processes to verify: • Personnel are aware of procedures for inspecting devices. • All devices are periodically inspected for evidence of tampering and unauthorized substitution.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of the inspection processes** for this testing procedure.	

PCI DSS Requirement					
9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**		**Reporting Details: Assessor's Response**		
9.5.1.2.1.a Examine the entity's targeted risk analysis for the frequency of periodic POI device inspections and type of inspections performed to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	**Identify** the evidence reference number(s) from Section 6 for the **entity's targeted risk analysis** examined for this testing procedure.				
9.5.1.2.1.b Examine documented results of periodic device inspections and interview personnel to verify that the frequency and type of POI device inspections performed match what is defined in the entity's targeted risk analysis conducted for this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented results of periodic device inspections** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement
9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
9.5.1.3.a Review training materials for personnel in POI environments to verify they include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **training materials** examined for this testing procedure.	
9.5.1.3.b Interview personnel in POI environments to verify they have received training and know the procedures for all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Requirement Description
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.

PCI DSS Requirement
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 10 are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 10 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
10.1.2.b Interview personnel with responsibility for performing activities in Requirement 10 to verify that roles and responsibilities are assigned as defined and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

PCI DSS Requirement
10.2.1 Audit logs are enabled and active for all system components and cardholder data.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.2.1 Interview the system administrator and examine system configurations to verify that audit logs are enabled and active for all system components.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

PCI DSS Requirement
10.2.1.1 Audit logs capture all individual user access to cardholder data.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.2.1.1 Examine audit log configurations and log data to verify that all individual user access to cardholder data is logged.	**Identify** the evidence reference number(s) from Section 6 for all **audit log configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **log data** examined for this testing procedure.	

PCI DSS Requirement
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.2.1.2 Examine audit log configurations and log data to verify that all actions taken by any individual with administrative access, including any interactive use of application or system accounts, are logged.	**Identify** the evidence reference number(s) from Section 6 for **all audit log configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **log data** examined for this testing procedure.	

PCI DSS Requirement
10.2.1.3 Audit logs capture all access to audit logs.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.2.1.3 Examine audit log configurations and log data to verify that access to all audit logs is captured.	**Identify** the evidence reference number(s) from Section 6 for all **audit log configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **log data** examined for this testing procedure.	

PCI DSS Requirement					
10.2.1.4 Audit logs capture all invalid logical access attempts.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.2.1.4 Examine audit log configurations and log data to verify that invalid logical access attempts are captured.	**Identify** the evidence reference number(s) from Section 6 for all **audit log configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **log data** examined for this testing procedure.	

PCI DSS Requirement
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.2.1.5 Examine audit log configurations and log data to verify that changes to identification and authentication credentials are captured in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **audit log configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **log data** examined for this testing procedure.	

PCI DSS Requirement					
10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
10.2.1.6 Examine audit log configurations and log data to verify that all elements specified in this requirement are captured.	**Identify** the evidence reference number(s) from Section 6 for all **audit log configurations** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **log data** examined for this testing procedure.				

PCI DSS Requirement					
10.2.1.7 Audit logs capture all creation and deletion of system-level objects.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
10.2.1.7 Examine audit log configurations and log data to verify that creation and deletion of system level objects is captured.	**Identify** the evidence reference number(s) from Section 6 for all **audit log configurations** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **log data** examined for this testing procedure.				

PCI DSS Requirement
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.2.2 Interview personnel and examine audit log configurations and log data to verify that all elements specified in this requirement are included in log entries for each auditable event (from 10.2.1.1 through 10.2.1.7).	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **audit log configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **log data** examined for this testing procedure.	

Requirement Description
10.3 Audit logs are protected from destruction and unauthorized modifications.

PCI DSS Requirement
10.3.1 Read access to audit logs files is limited to those with a job-related need.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.3.1 Interview system administrators and examine system configurations and privileges to verify that only individuals with a job-related need have read access to audit log files.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configurations and privileges** examined for this testing procedure.	

PCI DSS Requirement					
10.3.2 Audit log files are protected to prevent modifications by individuals.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
10.3.2 Examine system configurations and privileges and interview system administrators to verify that current audit log files are protected from modifications by individuals via access control mechanisms, physical segregation, and/or network segregation.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations and privileges** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement
10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.3.3 Examine backup configurations or log files to verify that current audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	**Identify** the evidence reference number(s) from Section 6 for all **backup configurations or log files** examined for this testing procedure.	

PCI DSS Requirement					
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.3.4 Examine system settings, monitored files, and results from monitoring activities to verify the use of file integrity monitoring or change-detection software on audit logs.	**Identify** the evidence reference number(s) from Section 6 for all **system settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **monitored files** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **results from monitoring activities** examined for this testing procedure.	

Requirement Description
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

PCI DSS Requirement
10.4.1 The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.4.1.a Examine security policies and procedures to verify that processes are defined for reviewing all elements specified in this requirement at least once daily.	**Identify** the evidence reference number(s) from Section 6 for all **security policies and procedures** examined for this testing procedure.	

10.4.1.b Observe processes and interview personnel to verify that all elements specified in this requirement are reviewed at least once daily	**Identify** the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
10.4.1.1 Automated mechanisms are used to perform audit log reviews. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
10.4.1.1 Examine log review mechanisms and interview personnel to verify that automated mechanisms are used to perform log reviews.	**Identify** the evidence reference number(s) from Section 6 for all **log review mechanisms** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
10.4.2.a Examine security policies and procedures to verify that processes are defined for reviewing logs of all other system components periodically.	**Identify** the evidence reference number(s) from Section 6 for all **security policies and procedures** examined for this testing procedure.				
10.4.2.b Examine documented results of log reviews and interview personnel to verify that log reviews are performed periodically.	**Identify** the evidence reference number(s) from Section 6 for all **documented results of log reviews** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1 ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
10.4.2.1.a Examine the entity's targeted risk analysis for the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.	**Identify** the evidence reference number(s) from Section 6 for the **entity's targeted risk analysis** examined for this testing procedure.				
10.4.2.1.b Examine documented results of periodic log reviews of all other system components (not defined in Requirement 10.4.1) and interview personnel to verify log reviews are performed at the frequency specified in the entity's targeted risk analysis performed for this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented results of all other system components (not defined in Requirement 10.4.1)** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
10.4.3 Exceptions and anomalies identified during the review process are addressed.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
10.4.3.a Examine security policies and procedures to verify that processes are defined for addressing exceptions and anomalies identified during the review process.	**Identify** the evidence reference number(s) from Section 6 for all **security policies and procedures** examined for this testing procedure.				
10.4.3.b Observe processes and interview personnel to verify that, when exceptions and anomalies are identified, they are addressed.	**Identify** the evidence reference number(s) from Section 6 for all **observations of processes** for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

Requirement Description
10.5 Audit log history is retained and available for analysis.

PCI DSS Requirement
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.5.1.a Examine documentation to verify that the following is defined: • Audit log retention policies. • Procedures for retaining audit log history for at least 12 months, with at least the most recent three months immediately available online.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

10.5.1.b Examine configurations of audit log history, interview personnel and examine audit logs to verify that audit logs history is retained for at least 12 months.	**Identify** the evidence reference number(s) from Section 6 for all **configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **audit logs** examined for this testing procedure.	
10.5.1.c Interview personnel and observe processes to verify that at least the most recent three months' audit log history is immediately available for analysis.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for the **observations of processes** for this testing procedure.	

Requirement Description
10.6 Time-synchronization mechanisms support consistent time settings across all systems.

PCI DSS Requirement
10.6.1 System clocks and time are synchronized using time-synchronization technology.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.6.1 Examine system configuration settings to verify that time-synchronization technology is implemented and kept current.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

PCI DSS Requirement
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.6.2 Examine system configuration settings for acquiring, distributing, and storing the correct time to verify the settings are configured in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

PCI DSS Requirement					
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
10.6.3.a Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations and time-synchronization settings** examined for this testing procedure.				
10.6.3.b Examine system configurations and time synchronization settings and logs and observe processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations time synchronization settings** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **logs** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for the **observations of processes** for this testing procedure.				

Requirement Description

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

PCI DSS Requirement

10.7.1 ***Additional requirement for service providers only*:** Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

- Network security controls.
- IDS/IPS.
- FIM.
- Anti-malware solutions.
- Physical access controls.
- Logical access controls.
- Audit logging mechanisms.
- Segmentation controls (if used).

Note: *This requirement will be* ***superseded*** *by Requirement 10.7.2 as of* ***31 March 2025****.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.7.1.a *Additional testing procedure for service provider assessments only:* Examine documentation to verify that processes are defined for the prompt detection and addressing of failures of critical security control systems, including but not limited to failure of all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
10.7.1.b *Additional testing procedure for service provider assessments only:* Observe detection and alerting processes and interview personnel to verify that failures of critical security control systems are detected and reported, and that failure of a critical security control results in the generation of an alert.	**Identify** the evidence reference number(s) from Section 6 for all **observations of detection and alerting processes** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used). ***Note:*** *This requirement applies to all entities, including service providers, and will supersede Requirements 10.7.1 as of 31 March 2025. It includes two additional critical security control systems not in Requirement 10.7.1. This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment and will supersede Requirement 10.7.1.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.7.2.a Examine documentation to verify that processes are defined for the prompt detection and addressing of failures of critical security control systems, including but not limited to failure of all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
10.7.2.b Observe detection and alerting processes and interview personnel to verify that failures of critical security control systems are detected and reported, and that failure of a critical security control results in the generation of an alert.	**Identify** the evidence reference number(s) from Section 6 for all **observations of detection and alerting processes** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
10.7.3 Failures of any critical security control systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls. ***Note:*** *This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a* ***best practice*** *for all other entities until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
10.7.3.a Examine documentation and interview personnel to verify that processes are defined and implemented to respond to a failure of any critical security control system and include at least all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

10.7.3.b Examine records to verify that failures of critical security control systems are documented to include: • Identification of cause(s) of the failure. • Duration (date and time start and end) of the security failure. • Details of the remediation required to address the root cause.	**Identify** the evidence reference number(s) from Section 6 for all **records** examined for this testing procedure.	

Requirement 11: Test Security of Systems and Networks Regularly

Requirement Description
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

PCI DSS Requirement
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures are managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
11.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 11 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
11.1.2.b Interview personnel with responsibility for performing activities in Requirement 11 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

Requirement Description
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

PCI DSS Requirement
11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.2.1.a Examine policies and procedures to verify processes are defined for managing both authorized and unauthorized wireless access points with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	

11.2.1.b Examine the methodology(ies) in use and the resulting documentation, and interview personnel to verify processes are defined to detect and identify both authorized and unauthorized wireless access points in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **methodology(ies) in use and resulting documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
11.2.1.c Examine wireless assessment results and interview personnel to verify that wireless assessments were conducted in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **wireless assessment results** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
11.2.1.d If automated monitoring is used, examine configuration settings to verify the configuration will generate alerts to notify personnel.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.	

PCI DSS Requirement					
11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
11.2.2 Examine documentation to verify that an inventory of authorized wireless access points is maintained, and a business justification is documented for all authorized wireless access points.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				

Requirement Description
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

PCI DSS Requirement
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.3.1.a Examine internal scan report results from the last 12 months to verify that internal scans occurred at least once every three months in the most recent 12-month period.	**Identify** the evidence reference number(s) from Section 6 for all **internal scan report results** examined for this testing procedure.	

11.3.1.b Examine internal scan report results from each scan and rescan run in the last 12 months to verify that all high-risk vulnerabilities and all critical vulnerabilities (defined in PCI DSS Requirement 6.3.1) are resolved.	**Identify** the evidence reference number(s) from Section 6 for all **internal scan report results** examined for this testing procedure.	
11.3.1.c Examine scan tool configurations and interview personnel to verify that the scan tool is kept up to date with the latest vulnerability information.	**Identify** the evidence reference number(s) from Section 6 for all **scan tool configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
11.3.1.d Interview responsible personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.3.1.1.a Examine the entity's targeted risk analysis that defines the risk for addressing all other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings at Requirement 6.3.1) to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.	**Identify** the evidence reference number(s) from Section 6 for the **entity's targeted risk analysis** examined for this testing procedure.	

11.3.1.1.b Interview responsible personnel and examine internal scan report results or other documentation to verify that all other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings at Requirement 6.3.1) are addressed based on the risk defined in the entity's targeted risk analysis, and that the scan process includes rescans as needed to confirm the vulnerabilities have been addressed.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **internal scan report results or other documentation** examined for this testing procedure.	

PCI DSS Requirement

11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows:

- Systems that are unable to accept credentials for authenticated scanning are documented.
- Sufficient privileges are used for those systems that accept credentials for scanning.
- If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.

Note: *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.3.1.2.a Examine scan tool configurations to verify that authenticated scanning is used for internal scans, with sufficient privileges, for those systems that accept credentials for scanning.	**Identify** the evidence reference number(s) from Section 6 for all **scan tool configurations** examined for this testing procedure.	
11.3.1.2.b Examine scan report results and interview personnel to verify that authenticated scans are performed.	**Identify** the evidence reference number(s) from Section 6 for all **examine scan report results** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
11.3.1.2.c If accounts used for authenticated scanning can be used for interactive login, examine the accounts and interview personnel to verify the accounts are managed following all elements specified in Requirement 8.2.2.	**Identify** the evidence reference number(s) from Section 6 for all **accounts** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
11.3.1.2.d Examine documentation to verify that systems that are unable to accept credentials for authenticated scanning are defined.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement
11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.3.1.3.a Examine change control documentation and internal scan reports to verify that system components were scanned after any significant changes.	**Identify** the evidence reference number(s) from Section 6 for all **change control documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **internal scan reports** examined for this testing procedure.	
11.3.1.3.b Interview personnel and examine internal scan and rescan reports to verify that internal scans were performed after significant changes and that all high-risk vulnerabilities and all critical vulnerabilities (defined in Requirement 6.3.1) were resolved.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **internal scan and rescan reports** examined for this testing procedure.	

11.3.1.3.c Interview personnel to verify that internal scans are performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach Appendix C to support this method.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.3.2.a Examine ASV scan reports from the last 12 months to verify that external vulnerability scans occurred at least once every three months in the most recent 12-month period.	**Identify** the evidence reference number(s) from Section 6 for all **ASV scan reports** examined for this testing procedure.	
11.3.2.b Examine the ASV scan report from each scan and rescan run in the last 12 months to verify that vulnerabilities are resolved and the ASV Program Guide requirements for a passing scan are met.	**Identify** the evidence reference number(s) from Section 6 for all **ASV scan report results** examined for this testing procedure.	
11.3.2.c Examine the ASV scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	**Identify** the evidence reference number(s) from Section 6 for all **ASV scan reports** examined for this testing procedure.	

PCI DSS Requirement
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.3.2.1.a Examine change control documentation and external scan reports to verify that system components were scanned after any significant changes.	**Identify** the evidence reference number(s) from Section 6 for all **change control documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **external scan reports** examined for this testing procedure.	
11.3.2.1.b Interview personnel and examine external scan and rescan reports to verify that external scans were performed after significant changes and that vulnerabilities scored 4.0 or higher by the CVSS were resolved.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **external scan and rescan reports** examined for this testing procedure.	

11.3.2.1.c Interview personnel to verify that external scans are performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

PCI DSS Requirement
11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.4.1 Examine documentation and interview personnel to verify that the penetration-testing methodology defined, documented, and implemented by the entity includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV)

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.4.2.a Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **scope of work** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for the **results from the most recent internal penetration test** examined for this testing procedure.	

11.4.2.b Interview personnel to verify that the internal penetration test was performed by a qualified internal resource or qualified external third-party and that organizational independence of the tester exists (not required to be a QSA or ASV).	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV)

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.4.3.a Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed according to all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **scope of work** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for the **results from the most recent external penetration test** examined for this testing procedure.	
11.4.3.b Interview personnel to verify that the external penetration test was performed by a qualified internal resource or qualified external third-party and that organizational independence of the tester exists (not required to be a QSA or ASV).	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.4.4 Examine penetration testing results to verify that noted exploitable vulnerabilities and security weaknesses were corrected in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **penetration testing results** examined for this testing procedure.	

PCI DSS Requirement
11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use • According to the entity's defined penetration testing methodology • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3) • Performed by a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV)

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.4.5.a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **segmentation controls** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for the **penetration testing methodology** examined for this testing procedure.	
11.4.5.b Examine the results from the most recent penetration test to verify the penetration test covers and addresses all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **results from the most recent penetration test** examined for this testing procedure.	

11.4.5.c Interview personnel to verify that the test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
11.4.6 ***Additional requirement for service providers only:*** If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.4.6.a *Additional testing procedure for service provider assessments only:* Examine the results from the most recent penetration test to verify that the penetration covers and addresses all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **results from the most recent penetration test** examined for this testing procedure.	
11.4.6.b *Additional testing procedure for service provider assessments only:* Interview personnel to verify that the test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
11.4.7 ***Additional requirement for multi-tenant service providers only:*** Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
11.4.7 ***Additional testing procedure for multi-tenant providers only:*** Examine evidence to verify that multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	**Identify** the evidence reference number(s) from Section 6 for all **evidence** examined for this testing procedure.				

Requirement Description
11.5 Network intrusions and unexpected file changes are detected and responded to.

PCI DSS Requirement
11.5.1 Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.5.1.a Examine system configurations and network diagrams to verify that intrusion-detection and/or intrusion-prevention techniques are in place to monitor all traffic: • At the perimeter of the CDE. • At critical points in the CDE.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **network diagrams** examined for this testing procedure.	

11.5.1.b Examine system configurations and interview responsible personnel to verify intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
11.5.1.c Examine system configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured to keep all engines, baselines, and signatures up to date.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **vendor documentation** examined for this testing procedure.	

PCI DSS Requirement

11.5.1.1 ***Additional requirement for service providers only:*** Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.

Note: *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.5.1.1.a *Additional testing procedure for service provider assessments only:* Examine documentation and configuration settings to verify that methods to detect and alert on/prevent covert malware communication channels are in place and operating.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.	
11.5.1.1.b *Additional testing procedure for service provider assessments only:* Examine the entity's incident-response plan (Requirement 12.10.1) to verify it requires and defines a response in the event that covert malware communication channels are detected.	**Identify** the evidence reference number(s) from Section 6 for the **entity's incident-response plan** examined for this testing procedure.	
11.5.1.1.c *Additional testing procedure for service provider assessments only:* Interview responsible personnel and observe processes to verify that personnel maintain knowledge of covert malware communication and control techniques and are knowledgeable about how to respond when malware is suspected.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of processes** conducted for this testing procedure.	

PCI DSS Requirement					
11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
11.5.2.a Examine system settings, monitored files, and results from monitoring activities to verify the use of a change-detection mechanism.	**Identify** the evidence reference number(s) from Section 6 for all **system settings** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **monitored files** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **results from monitoring activities** examined for this testing procedure.				
11.5.2.b Examine settings for the change-detection mechanism to verify it is configured in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **settings for the change-detection mechanism** examined for this testing procedure.				

Requirement Description

11.6 Unauthorized changes on payment pages are detected and responded to.

PCI DSS Requirement

11.6.1 A change- and tamper-detection mechanism is deployed as follows:

- To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the security-impacting HTTP headers and the script contents of payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP headers and payment pages.
- The mechanism functions are performed as follows:
  - At least once weekly

  OR
  - Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).

Note: *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
11.6.1.a Examine system settings, monitored payment pages, and results from monitoring activities to verify the use of a change- and tamper-detection mechanism.	**Identify** the evidence reference number(s) from Section 6 for all **system settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **monitoring activities** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **results from monitoring activities** examined for this testing procedure.	
11.6.1.b Examine configuration settings to verify the mechanism is configured in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.	
11.6.1.c If the mechanism functions are performed at an entity-defined frequency, examine the entity's targeted risk analysis for determining the frequency to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.	**Identify** the evidence reference number(s) from Section 6 for the **entity's targeted risk analysis** examined for this testing procedure.	
11.6.1.d Examine configuration settings and interview personnel to verify the mechanism functions are performed either: • At least once weekly OR • At the frequency defined in the entity's targeted risk analysis performed for this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **configuration settings** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

Requirement Description
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

PCI DSS Requirement
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.1.1 Examine the information security policy and interview personnel to verify that the overall information security policy is managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **information security policy** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
12.1.2 Examine the information security policy and interview responsible personnel to verify the policy is managed in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **information security policies** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.1.3.a Examine the information security policy to verify that they clearly define information security roles and responsibilities for all personnel.	**Identify** the evidence reference number(s) from Section 6 for the **information security policy** examined for this testing procedure.	
12.1.3.b Interview personnel in various roles to verify they understand their information security responsibilities.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
12.1.3.c Examine documented evidence to verify personnel acknowledge their information security responsibilities.	**Identify** the evidence reference number(s) from Section 6 for all **documented evidence** examined for this testing procedure.	

PCI DSS Requirement					
12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
12.1.4 Examine the information security policy to verify that information security is formally assigned to a Chief Information Security Officer or other information security-knowledgeable member of executive management.	**Identify** the evidence reference number(s) from Section 6 for the **information security policy** examined for this testing procedure.				

Requirement Description
12.2 Acceptable use policies for end-user technologies are defined and implemented.

PCI DSS Requirement
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.2.1 Examine the acceptable use policies for end-user technologies and interview responsible personnel to verify processes are documented and implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **acceptable use policies** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

PCI DSS Requirement

12.3.1 For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.

Note: *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected.

Note*: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*

**As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.3.1 Examine documented policies and procedures to verify a process is defined for performing targeted risk analyses for each PCI DSS requirement that specifies completion of a targeted risk analysis, and that the process includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented policies and procedures** examined for this testing procedure.	

PCI DSS Requirement
12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach Appendix C to support this method.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.3.2 Examine the documented targeted risk-analysis for each PCI DSS requirement that the entity meets with the customized approach to verify that documentation for each requirement exists and is in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • Documentation of a plan to respond to anticipated changes in cryptographic vulnerabilities. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.3.3 Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.3.4 Examine documentation for the review of hardware and software technologies in use and interview personnel to verify that the review is in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
12.4 PCI DSS compliance is managed.

PCI DSS Requirement
12.4.1 ***Additional requirement for service providers only:*** Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program and communication to executive management.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.4.1 ***Additional testing procedure for service provider assessments only:*** Examine documentation to verify that executive management has established responsibility for the protection of cardholder data and a PCI DSS compliance program in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement
12.4.2 ***Additional requirement for service providers only:*** Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.4.2.a ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify that processes are defined for conducting reviews to confirm that personnel are performing their tasks in accordance with all security policies and all operational procedures, including but not limited to the tasks specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	

12.4.2.b *Additional testing procedure for service provider assessments only:* Interview responsible personnel and examine records of reviews to verify that reviews are performed: • At least once every three months. • By personnel other than those responsible for performing the given task.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **records of reviews** examined for this testing procedure.	

PCI DSS Requirement
12.4.2.1 ***Additional requirement for service providers only:*** Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. • Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.4.2.1 ***Additional testing procedure for service provider assessments only:*** Examine documentation from the reviews conducted in accordance with PCI DSS Requirement 12.4.2 to verify the documentation includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

Requirement Description
12.5 PCI DSS scope is documented and validated.

PCI DSS Requirement
12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.5.1.a Examine the inventory to verify it includes all in-scope system components and a description of function/use for each.	**Identify** the evidence reference number(s) from Section 6 for the **inventory** examined for this testing procedure.	
12.5.1.b Interview personnel to verify the inventory is kept current.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.5.2.a Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least once every 12 months. • After significant changes to the in-scope environment.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

12.5.2.b Examine documented results of scope reviews performed by the entity to verify that PCI DSS scoping confirmation activity includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented results of scope reviews** examined for this testing procedure.	

PCI DSS Requirement					
12.5.2.1 ***Additional requirement for service providers only:*** PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**		**Reporting Details: Assessor's Response**		
12.5.2.1.a ***Additional testing procedure for service provider assessments only:*** Examine documented results of scope reviews and interview personnel to verify that reviews per Requirement 12.5.2 are performed: • At least once every six months, and • After significant changes	**Identify** the evidence reference number(s) from Section 6 for all **documented results of scope reviews** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

12.5.2.1.b *Additional testing procedure for service provider assessments only:* Examine documented results of scope reviews to verify that scoping validation includes all elements specified in Requirement 12.5.2.	**Identify** the evidence reference number(s) from Section 6 for all d**ocumented results of scope reviews** examined for this testing procedure.	

PCI DSS Requirement					
12.5.3 *Additional requirement for service providers only:* Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions		Reporting Details: Assessor's Response		
12.5.3.a *Additional testing procedure for service provider assessments only:* Examine policies and procedures to verify that processes are defined such that a significant change to organizational structure results in documented review of the impact to PCI DSS scope and applicability of controls.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.				

12.5.3.b *Additional testing procedure for service provider assessments only:* Examine documentation (for example, meeting minutes) and interview responsible personnel to verify that significant changes to organizational structure resulted in documented reviews that included all elements specified in this requirement, with results communicated to executive management.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
12.6 Security awareness education is an ongoing activity.

PCI DSS Requirement
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.6.1 Examine the security awareness program to verify it provides awareness to all personnel about the entity's information security policy and procedures, and personnel's role in protecting the cardholder data.	**Identify** the evidence reference number(s) from Section 6 for the **security awareness program** examined for this testing procedure.	

PCI DSS Requirement
12.6.2 The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's cardholder data and/or sensitive authentication data, or the information provided to personnel about their role in protecting cardholder data. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.6.2 Examine security awareness program content, evidence of reviews, and interview personnel to verify that the security awareness program is in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **security awareness program content** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **evidence of reviews** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
12.6.3.a Examine security awareness program records to verify that personnel attend security awareness training upon hire and at least once every 12 months.	**Identify** the evidence reference number(s) from Section 6 for all **security awareness program records** examined for this testing procedure.				
12.6.3.b Examine security awareness program materials to verify the program includes multiple methods of communicating awareness and educating personnel.	**Identify** the evidence reference number(s) from Section 6 for all **security awareness program materials** examined for this testing procedure.				
12.6.3.c Interview personnel to verify they have completed awareness training and are aware of their role in protecting cardholder data.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

12.6.3.d Examine security awareness program materials and personnel acknowledgments to verify that personnel acknowledge at least once every 12 months that they have read and understand the information security policy and procedures.	**Identify** the evidence reference number(s) from Section 6 for all **security awareness program materials** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **personnel acknowledgments** examined for this testing procedure.	

PCI DSS Requirement

12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of cardholder data and/or sensitive authentication data, including but not limited to:

- Phishing and related attacks.
- Social engineering.

Note: *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.6.3.1 Examine security awareness training content to verify it includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **security awareness training content** examined for this testing procedure.	

PCI DSS Requirement
12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.6.3.2 Examine security awareness training content to verify it includes awareness about acceptable use of end-user technologies in accordance with Requirement 12.2.1.	**Identify** the evidence reference number(s) from Section 6 for all **security awareness training content** examined for this testing procedure.	

Requirement Description
12.7 Personnel are screened to reduce risks from insider threats.

PCI DSS Requirement
12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.7.1 Interview responsible Human Resource department management to verify that screening is conducted, within the constraints of local laws, prior to hiring potential personnel who will have access to the CDE.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

Requirement Description
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

PCI DSS Requirement
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.8.1.a Examine policies and procedures to verify that processes are defined to maintain a list of TPSPs, including a description for each of the services provided, for all TPSPs with whom account data is shared or that could affect the security of account data.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
12.8.1.b Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement
12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.8.2.a Examine policies and procedures to verify that processes are defined to maintain written agreements with all TPSPs in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
12.8.2.b Examine written agreements with TPSPs to verify they are maintained in accordance with all elements as specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **written agreements** examined for this testing procedure.	

PCI DSS Requirement					
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.8.3.a Examine policies and procedures to verify that processes are defined for engaging TPSPs, including proper due diligence prior to engagement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
12.8.3.b Examine evidence and interview responsible personnel to verify the process for engaging TPSPs includes proper due diligence prior to engagement.	**Identify** the evidence reference number(s) from Section 6 for all **evidence** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.8.4.a Examine policies and procedures to verify that processes are defined to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
12.8.4.b Examine documentation and interview responsible personnel to verify that the PCI DSS compliance status of each TPSP is monitored at least once every 12 months.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
12.8.5.a Examine policies and procedures to verify that processes are defined to maintain information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both the TPSP and the entity.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.				
12.8.5.b Examine documentation and interview personnel to verify the entity maintains information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both entities.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

Requirement Description
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

PCI DSS Requirement
12.9.1 ***Additional requirement for service providers only:*** TPSPs provide written agreements to customers that include acknowledgements that TPSPs are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that the TPSP could impact the security of the customer's cardholder data and/or sensitive authentication data.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.9.1 ***Additional testing procedure for service provider assessments only:*** Examine TPSP policies, procedures, and templates used for written agreements to verify processes are defined for the TPSP to provide written acknowledgments to customers in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **TPSP policies, procedures, and templates used for written agreements** examined for this testing procedure.	

PCI DSS Requirement
12.9.2 ***Additional requirement for service providers only:*** TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5), for any service the TPSP provides that meets a PCI DSS requirement(s) on behalf of customers or that can impact security of customers' cardholder data and/or sensitive authentication data.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.9.2 ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify processes are defined for the TPSPs to support customers' request for information to meet Requirements 12.8.4 and 12.8.5 in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	

Requirement Description

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

PCI DSS Requirement

12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:

- Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
- Incident response procedures with specific containment and mitigation activities for different types of incidents.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected.

***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*

**As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.10.1.a Examine the incident response plan to verify that the plan exists and includes at least the elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **incident response plans** examined for this testing procedure.	

12.10.1.b Interview personnel and examine documentation from previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement

12.10.2 At least once every 12 months, the security incident response plan is:

- Reviewed and the content is updated as needed.
- Tested, including all elements listed in Requirement 12.10.1.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.10.2 Interview personnel and review documentation to verify that, at least once every 12 months, the security incident response plan is: • Reviewed and updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement

12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.10.3 Examine documentation and interview responsible personnel occupying designated roles to verify that specific personnel are designated to be available on a 24/7 basis to respond to security incidents.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement					
12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
12.10.4 Examine training documentation and interview incident response personnel to verify that personnel are appropriately and periodically trained on their incident response responsibilities.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement					
12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
12.10.4.1.a Examine the entity's targeted risk analysis for the frequency of training for incident response personnel to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	**Identify** the evidence reference number(s) from Section 6 for the **entity's targeted risk analysis** examined for this testing procedure.				
12.10.4.1.b Examine documented results of periodic training of incident response personnel and interview personnel to verify training is performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documented results** examined for this testing procedure.				
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.				

PCI DSS Requirement
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. *This bullet is a **best practice** until **31 March 2025**, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.* • Detection of unauthorized wireless access points.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.10.5 Examine documentation and observe incident response processes to verify that monitoring and responding to alerts from security monitoring systems are covered in the security incident response plan, including but not limited to the systems specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **observations of incident response processes** for this testing procedure.	

PCI DSS Requirement					
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.10.6.a Examine policies and procedures to verify that processes are defined to modify and evolve the security incident response plan according to lessons learned and to incorporate industry developments.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.	
12.10.6.b Examine the security incident response plan and interview responsible personnel to verify that the incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	**Identify** the evidence reference number(s) from Section 6 for the **security incident response plan** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
12.10.7.a Examine documented incident response procedures to verify that procedures for responding to the detection of stored PAN anywhere it is not expected to exist, ready to be initiated, and include all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented incident response procedures** examined for this testing procedure.	

12.10.7.b Interview personnel and examine records of response actions to verify that incident response procedures are performed upon detection of stored PAN anywhere it is not expected.	**Identify** the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **records of response actions** examined for this testing procedure.	

Appendix A Additional PCI DSS Requirements

A1 Additional PCI DSS Requirements for Multi-Tenant Service Providers

Requirement Description
A1.1 Multi-tenant service providers protect and separate all customer environments and data.

PCI DSS Requirement
A1.1.1 Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization. • Customers cannot access the provider's environment without authorization. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A1.1.1 Examine documentation and system and network configurations and interview personnel to verify that logical separation is implemented in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system and network configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

PCI DSS Requirement
A1.1.2 Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A1.1.2.a Examine documentation to verify controls are defined such that each customer only has permission to access its own cardholder data and CDE.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
A1.1.2.b Examine system configurations to verify that customers have privileges established to only access their own account data and CDE.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	

PCI DSS Requirement					
A1.1.3 Controls are implemented such that each customer can only access resources allocated to them.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A1.1.3 Examine customer privileges to verify each customer can only access resources allocated to them.	**Identify** the evidence reference number(s) from Section 6 for all **customer privileges** examined for this testing procedure.	

PCI DSS Requirement					
A1.1.4 The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing. ***Note:*** *This requirement is a* ***best practice until 31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A1.1.4 Examine the results from the most recent penetration test to verify that testing confirmed the effectiveness of logical separation controls used to separate customer environments.	**Identify** the evidence reference number(s) from Section 6 for the **results from the most recent penetration test** examined for this testing procedure.	

Requirement Description
A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.

PCI DSS Requirement
A1.2.1 Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review only by the owning customer. • Log locations are clearly communicated to the owning customer. • Log data and availability is consistent with PCI DSS Requirement 10.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A1.2.1 Examine documentation and system configuration settings to verify the provider has enabled audit log capability for each customer environment in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **system configuration settings** examined for this testing procedure.	

PCI DSS Requirement					
A1.2.2 Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response			
A1.2.2 Examine documented procedures to verify that the provider has processes or mechanisms to support and/or facilitate a prompt forensic investigation of related servers in the event of a suspected or confirmed security incident for any customer.	**Identify** the evidence reference number(s) from Section 6 for the **documented procedures** examined for this testing procedure.				

PCI DSS Requirement
A1.2.3 Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: • Customers can securely report security incidents and vulnerabilities to the provider. • The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1. ***Note:*** *This requirement is a* ***best practice*** *until* ***31 March 2025****, after which it will be required and must be fully considered during a PCI DSS assessment.*

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note****: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*	

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A1.2.3 Examine documented procedures and interview personnel to verify that the provider has a mechanism for reporting and addressing suspected or confirmed security incidents and vulnerabilities, in accordance with all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented procedures** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **interviews** conducted for this testing procedure.	

A2 Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections

Requirement Description
A2.1 POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits.

PCI DSS Requirement
A2.1.1 Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**

Describe why the assessment finding was selected.

***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*

** As applicable, complete and attach Appendix C to support this method.*

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A2.1.1 For POS POI terminals using SSL and/or early TLS, confirm the entity has documentation (for example, vendor documentation, system/network configuration details) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

PCI DSS Requirement
A2.1.2 ***Additional requirement for service providers only:*** All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes: • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment. • Risk-assessment results and risk-reduction controls in place. • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS. • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments. • Overview of migration project plan to replace SSL/early TLS at a future date.

Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* *** As applicable, complete and attach Appendix C to support this method.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A2.1.2 ***Additional testing procedure for service provider assessments only*:** Review the documented Risk Mitigation and Migration Plan to verify it includes all elements specified in this requirement.	**Identify** the evidence reference number(s) from Section 6 for the **documented Risk Mitigation and Migration Plan** examined for this testing procedure.	

PCI DSS Requirement					
A2.1.3 ***Additional requirement for service providers only:*** All service providers provide a secure service offering.					
Assessment Findings (select one)				Select If Below Method(s) Was Used	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach**
☐	☐	☐	☐	☐	**N/A**
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* ** As applicable, complete and attach Appendix C to support this method.*					

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
A2.1.3 ***Additional testing procedure for service provider assessments only:*** Examine system configurations and supporting documentation to verify the service provider offers a secure protocol option for its service.	**Identify** the evidence reference number(s) from Section 6 for all **system configurations** examined for this testing procedure.	
	Identify the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	

A3 Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements.

Entities that are required to validate to these requirements should refer to the following documents for reporting:

- PCI DSS v4.0.1 Supplemental Report on Compliance Template - Designated Entities Supplemental Validation
- PCI DSS v4.0.1 Supplemental Attestation of Compliance for Report on Compliance - Designated Entities Supplemental Validation

These documents are available in the PCI SSC Document Library.

Note that an entity is ONLY required to undergo an assessment according to this Appendix if instructed to do so by an acquirer or a payment brand.

Appendix B Compensating Controls

Compensating controls may be considered when an entity cannot meet a PCI DSS requirement explicitly as stated, due to legitimate and documented technical or business constraints but has sufficiently mitigated the risk associated with not meeting the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. To understand the intent of a requirement, see the Customized Approach Objective for most PCI DSS requirements. If a requirement is not eligible for the Customized Approach and therefore does not have a Customized Approach Objective, refer to the Purpose in the Guidance column for that requirement.
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)
4. When evaluating "above and beyond" for compensating controls, consider the following:

Note: *All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS assessment. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a given compensating control will not be effective in all environments.*

a. Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting cleartext administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for the lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of cleartext passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

b. Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area but are not required for the item under review.

c. Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to address a vulnerability that is exploitable through a network interface because a security update is not yet available from a vendor, a compensating control could consist of controls that include all of the following: 1) internal network segmentation, 2) limiting network access to the vulnerable interface to only required devices (IP address or MAC address filtering), and 3) IDS/IPS monitoring of all traffic destined to the vulnerable interface.

5. Address the additional risk imposed by not adhering to the PCI DSS requirement.
6. Address the requirement currently and in the future. A compensating control cannot address a requirement that was missed in the past (for example, where the performance of a task was required two quarters ago, but that task was not performed).

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to confirm that each compensating control adequately addresses the risk that the original PCI DSS requirement was designed to address, per items 1-6 above.

To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete. Additionally, compensating control results must be documented in the applicable report for the assessment (for example, a Report on Compliance or a Self-Assessment Questionnaire) in the corresponding PCI DSS requirement section, and included when the applicable report is submitted to the requesting organization.

Appendix C Compensating Controls Worksheet

Use this worksheet to document any instance where a compensating control is used to meet a PCI DSS defined requirement. Note that compensating controls must also be documented at the corresponding PCI DSS requirement in Part II, section 7 Findings and Observations.

Note: *Only entities that have legitimate and documented technological or business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	
2. Definition of Compensating Controls	Define the compensating controls, explain how they address the objectives of the original control and the increased risk, if any.	
3. Objective	Define the objective of the original control (for example, the Customized Approach Objective).	
	Identify the objective met by the compensating control (*note: this can be, but is not required to be, the stated Customized Approach Objective for the PCI DSS requirement*).	
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	

Appendix D Customized Approach

This approach is intended for entities that decide to meet a PCI DSS requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. The customized approach allows an entity to take a strategic approach to meeting a requirement's Customized Approach Objective, so it can determine and design the security controls needed to meet the objective in a manner unique for that organization.

The entity implementing a customized approach must satisfy the following criteria:

- Document and maintain evidence about each customized control, including all information specified in the Controls Matrix Template in *PCI DSS v4.x: Sample Templates to Support Customized Approach on the PCI SSC website*.
- Perform and document a targeted risk analysis (PCI DSS Requirement 12.3.2) for each customized control, including all information specified in the Targeted Risk Analysis Template in PCI DSS v4.x: Sample Templates to Support Customized Approach on the PCI SSC website.
- Perform testing of each customized control to prove effectiveness, and document testing performed, methods used, what was tested, when testing was performed, and results of testing in the controls matrix.
- Monitor and maintain evidence about the effectiveness of each customized control.
- Provide completed controls matrix(es), targeted risk analysis, testing evidence, and evidence of customized control effectiveness to its assessor.

The assessor performing an assessment of customized controls must satisfy the following criteria:

- Review the entity's controls matrix(es), targeted risk analysis, and evidence of control effectiveness to fully understand the customized control(s) and to verify the entity meets all Customized Approach documentation and evidence requirements.
- Derive and document the appropriate testing procedures needed to conduct thorough testing of each customized control.
- Test each customized control to determine whether the entity's implementation 1) meets the requirement's Customized Approach Objective and 2) results in an "in place" finding for the requirement.
- At all times, QSAs maintain independence requirements defined in the QSA Qualification Requirements. This means if a QSA is involved in designing or implementing a customized control, that QSA does not also derive testing procedures for, assess, or assist with the assessment of that customized control.

The entity and its assessor are expected to work together to ensure 1) they agree that the customized control(s) fully meets the customized approach objective, 2) the assessor fully understands the customized control, and 3) the entity understands the derived testing the assessor will perform.

Use of the customized approach must be documented by a QSA or ISA in accordance with instructions in the Report on Compliance (ROC) Template and following the instructions in the *FAQs for use with PCI DSS v4.x ROC Template* available on the PCI SSC website.

Entities that complete a Self-Assessment Questionnaire are not eligible to use a customized approach; however, these entities may elect to have a QSA or ISA perform their assessment and document it in a ROC Template.

The use of the customized approach may be regulated by organizations that manage compliance programs (for example, payment brands and acquirers). Therefore, questions about use of a customized approach must be referred to those organizations, including, for example, whether an entity is required to use a QSA, or may use an ISA to complete an assessment using the customized approach.

Note: *Compensating controls are not an option with the customized approach. Because the customized approach allows an entity to determine and design the controls needed to meet a requirement's Customized Approach Objective, the entity is expected to effectively implement the controls it designed for that requirement without needing to also implement alternate, compensating controls.*

Appendix E Customized Approach Template

Use this template to document each instance where a customized control is used to meet a PCI DSS requirement. Note that each use of the Customized Approach must also be documented at the corresponding PCI DSS requirement in Part II, section 7 Findings and Observations.

Requirement Number and Definition:

Identify the **customized control name / identifier** for each control used to meet the Customized Approach Objective. *(**Note:** use the Customized Control name from the assessed entity's controls matrix)*	
Describe each control used to meet the Customized Approach Objective. *(**Note**: Refer to the Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures for the Customized Approach Objective)*	
Describe how the control(s) meet the Customized Approach Objective.	
Identify the **Controls Matrix documentation** reviewed that supports a customized approach for this requirement.	
Identify the **Targeted Risk Analysis documentation** reviewed that supports the customized approach for this requirement.	
Identify name(s) of the assessor(s) who attests that: • The entity completed the Controls Matrix including all information specified in the Controls Matrix Template in *PCI DSS v4.x: Sample Templates to Support Customized Approach on the PCI SSC website,* and the results of the Controls Matrix support the customized approach for this requirement. • The entity completed the Targeted Risk Analysis including all information specified in the Targeted Risk Analysis Template in *PCI DSS v4.x: Sample Templates to Support Customized Approach on the PCI SSC website*, and that the results of the Risk Analysis support use of the customized approach for this requirement.	

Describe the testing procedures derived and performed by the assessor to validate that the **implemented controls meet the Customized Approach Objective**; for example, whether the customized control(s) is sufficiently robust to provide at least an equivalent level of protection as provided by the defined approach. ***Note 1:*** *Technical reviews (for example, reviewing configuration settings, operating effectiveness, etc.) should be performed where possible and appropriate.* ***Note 2:*** *Add additional rows for each assessor-derived testing procedure, as needed. Ensure that all rows to the right of the "Assessor-derived testing procedure" are copied for each assessor-derived testing procedure that is added.*		
Enter assessor-derived testing procedure here:	**Identify** what was tested (for example, individuals interviewed, system components reviewed, processes observed, etc.) ***Note:*** *all items tested must be uniquely identified.*	
	Identify all evidence examined for this testing procedure.	
	Describe the results of the testing performed by the assessor for this testing procedure and how these results verify the implemented controls meet the Customized Approach Objective.	

Document the testing procedures derived and performed by the assessor to validate **the controls are maintained to ensure ongoing effectiveness**; for example, how the entity monitors for control effectiveness and how control failures are detected, responded to, and the actions taken. ***Note 1:*** *Technical reviews (for example, reviewing configuration settings, operating effectiveness, etc.) should be performed where possible and appropriate.* ***Note 2:*** *Add additional rows for each assessor-derived testing procedure, as needed. Ensure that all rows to the right of the "Assessor-derived testing procedure" are copied for each assessor-derived testing procedure that is added.*		
Enter assessor-derived testing procedure here:	**Identify** what was tested (for example, individuals interviewed, system components reviewed, processes observed, etc.) ***Note****: all items tested must be uniquely identified.*	
	Identify all evidence examined for this testing procedure.	
	Describe the results of the testing performed by the assessor for this testing procedure and how these results verify the implemented controls are maintained to ensure ongoing effectiveness.	