Payment Card Industry (PCI)
Software Security Framework

Secure Software Template for Report on Validation

Version 1.2

April 2023

Document Changes

Date	Version	Description
September 2019	1.0	Initial release of the Report on Validation (ROV) template for the *PCI Secure Software Requirements and Assessment Procedures,* version 1.0.
April 2021	1.1	Updates to align with changes to the *PCI Software Security Framework – Secure Software Requirements and Assessment Procedures* from version 1.0 to version 1.1. Also includes minor corrections and edits made for clarification and/or formatting purposes and to address errata.
April 2023	1.2	Updates to align with changes to the *PCI Software Security Framework – Secure Software Requirements and Assessment Procedures* from version 1.1 to version 1.2.

Table of Contents

Introduction to the PCI Secure Software Report on Validation Template

This document, the *PCI Software Security Framework – Secure Software Template for Report on Validation* (Secure Software ROV Template) is for use with the *PCI Software Security Framework – Secure Software Requirements and Assessment Procedures* (Secure Software Standard) Version 1.2.

It is the mandatory template for Secure Software Assessors completing a Secure Software Assessment.

A Secure Software Assessment involves thorough testing and assessment activities from which the assessor generates detailed workpapers for each control objective and its associated test requirements. These workpapers contain records of the assessment activities, including observations, configurations, process information, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the assessment. The Secure Software Report on Validation (ROV) acts as a comprehensive summary of the testing activities performed and the information that is collected during the Secure Software Assessment. The information contained in a Secure Software ROV must provide enough detail and coverage to support the assessor's opinion that the validated software has met all control objectives within the PCI Secure Software Standard.

Using this Document

The PCI Secure Software Report on Validation Template provides reporting instructions and a reporting template for Secure Software Assessors. This template assures a consistent level of reporting against the PCI Secure Software Standard for all assessors.

Tables have been included in this template to assist with the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase or decrease the number of rows or to change column width. Additional appendices may be added if there is relevant information that is not addressed in the current template. However, the assessor must not remove any details from the tables provided in this document. Minor customizations, such as the addition of company logos, are acceptable.

Do not delete any content from the Secure Software ROV Template. The Introduction section of this document may be deleted, but the assessor must follow the instructions in this section while documenting the assessment.

All numbered sections must be thoroughly and accurately completed. The Secure Software ROV Template also contains instructions to help ensure that Secure Software Assessors supply all required information for each section. All responses should be entered in the applicable location or table provided in the template. Responses should be specific, but efficient. Details provided should focus on the quality of detail, rather than lengthy, repeated text. Copying text from the control objectives or test requirements is discouraged, as it does not add any level of assurance to the narrative. Use of template language for summaries and descriptions is also discouraged and details should be specifically relevant to the assessed software.

Related Publications

This template is to be used in conjunction with the appropriate versions of the following PCI Software Security Framework documents, available on the PCI SSC website at https://www.pcisecuritystandards.org.

- *PCI Software Security Framework – Secure Software Requirements and Assessment Procedures* (Secure Software Standard).
- *PCI Software Security Framework – Secure Software Program Guide* (Secure Software Program Guide)
- *PCI Software Security Framework – Secure Software Attestation of Validation* (Secure Software AOV)
- *PCI Software Security Framework – Glossary of Terms, Abbreviations, and Acronyms* (SSF Glossary)
- *PCI Software Security Framework – Qualification Requirements for SSF Assessors* (SSF Assessor Qualification Requirements)

Documenting the Assessment Findings and Observations

The results of the Secure Software Assessment are documented within the Detailed Findings and Observations section of the Secure Software ROV Template. An example layout of the Detailed Findings and Observations section is provided in Table 1.

Table 1. Detailed Findings and Observations

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 1: Control Objective Title Parent Control Objective Summary		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
1.1 Child Control Objective Summary		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
1.1.a Test Requirement	**R1** Reporting Instruction			
	R2 Reporting Instruction			

For the Summary of Assessment Findings, there are three results possible—In Place, Not in Place, and N/A (Not Applicable). Only one selection is to be made for each control objective. Table 2 provides a helpful representation when considering which selection to make. Reporting details and results should be consistent throughout the ROV, as well as consistent with other related reporting materials, such as the Attestation of Validation (AOV).

Table 2. Selecting the Appropriate Validation Result

Response	When to use this response:
In Place	The expected testing has been performed and all elements of the control objective have been met. Detailed testing must be performed and reporting provided that demonstrates how the assessor confirmed the control objective is In Place.
Not in Place	Some or all elements of the control objective have not been met, are in the process of being implemented, or require further testing before it will be known whether they are in place.
N/A (Not Applicable)	The control objective does not apply to the assessed software or software vendor. All "N/A" responses require detailed reporting on the testing performed and the results of the tests that explain why the control objective does not apply. **In general, all control objectives within a given module must be satisfied and cannot be marked as N/A**, unless there are legitimate technical constraints that exist that prevent the control objective from being met. Where third-party features or functions are relied upon to satisfy a particular control objective, the third-party features and functions must be included in the Secure Software Assessment to confirm that the configuration and use of such features and functions does not expose vulnerabilities.

Understanding the Reporting Instructions

In addition to specifying whether a control objective is "In Place," "Not in Place," or "N/A," the Secure Software Assessor must also document their findings for each test requirement. One or more reporting instructions are provided for each test requirement. Responses are required for all reporting instructions except where explicitly noted within the reporting instruction itself.

To provide consistency in how Secure Software Assessors document their findings, the reporting instructions use standardized terms. Those terms and the context in which they should be interpreted are provided in Table 3.

Table 3. Reporting Instruction Terms and Response Formats

Reporting Instruction Term	Example Usage	Description of Response
Describe	Describe each of the software tests performed to identify the transaction types and card data elements supported by the software.	The response would include a detailed description of the item or activity in question – for example, details of how evidence examined and/or individuals interviewed demonstrate a control objective was met, or how the assessor concluded an implemented security control 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.
Identify	Identify the evidence obtained that details all configuration options provided by the software.	The response would be a brief overview or descriptive list of the applicable items – for example: the titles of documents that were examined or generated by the assessor, a list of vulnerabilities that were tested, or the names and job titles of individuals who were interviewed.
Indicate	Indicate whether any functions expose methods or services which have publicly disclosed vulnerabilities (yes/no).	The response would be either "Yes" or "No." ***Note**: The applicability of some reporting instructions may be dependent on the response of a previous reporting instruction. For example, a response of "yes" to a question about a Secure Software control may result in further details being requested about that control. If applicable, the reporting instruction will direct the assessor to a subsequent instruction based on the yes/no answer.*

While it is expected that a Secure Software Assessor will report their findings for each test requirement, it may be necessary for a control objective to be validated using methods other than or in addition to those stated in the test requirements. In such cases, the Secure Software Assessor should describe why alternative assessment procedures were used and how those assessment procedures provide at least the same level of assurance as the original test requirements.

Reporting Expectations

DO:	DO NOT:
• Complete all sections in the order specified, with concise detail. • Read and understand the intent of each control objective and test requirement. • Provide a response for every reporting instruction. • Provide sufficient detail, information, and rationale to demonstrate a finding of "In Place" or "N/A." • Describe how a control objective was verified as the reporting instruction directs, not just that it was verified. • Ensure that all parts of the test requirements and reporting instructions are addressed. • Ensure the response covers all applicable systems, processes, components, APIs, and functions including those provided by third parties. • Perform an internal quality assurance review of the ROV for clarity, accuracy, and quality. • Provide useful, meaningful diagrams, as directed. • Provide full dates where dates are required, using the "dd-mm-yyyy" format consistently throughout the document.	• Do not report items as "In Place" unless they have been verified as being "In Place." • Do not include forward-looking statements or project plans in the "In Place" column. • Do not simply repeat or echo the test requirements in the response. • Do not copy responses from one test requirement to another. • Do not copy responses from previous assessments. • Do not include information irrelevant to the assessment.

Use of Sampling During Testing

Where appropriate or instructed, Secure Software Assessors may utilize sampling as part of the testing process. If sampling is used, the Secure Software Assessor must summarize their sampling methodology and specify each sample set used in Section 3.4, "Sampling" of the *Secure Software ROV Reporting Template* rather than list out the items from the sample within the individual reporting instruction response.

Using the Appendices

The Secure Software ROV Reporting Template includes two appendices:

- Appendix A, Additional Information Worksheet
- Appendix B, Testing Environment Configuration for Secure Software Assessments

Appendix A is optional and may be used to add extra information to support the assessment findings if the information is too large to fit in the Assessor's Findings column within the Detailed Findings and Observations section. Examples of information that may be added in Appendix A include diagrams, flowcharts, or tables that support the Secure Software Assessor's findings. Any information recorded in Appendix A should reference back to the applicable Secure Software Standard control objectives and test requirements.

Appendix B is mandatory and must be used to confirm that the environment used by the assessor to conduct the Secure Software Assessment was configured in accordance with Section 4.6.1 of the *Secure Software Program Guide*. This confirmation must be submitted to PCI SSC along with the completed *Report on Validation (ROV)*.

Note: *Additional appendices may be added if there is material relevant to the Secure Software Assessment that does not fit within the current template format.*

PCI Secure Software Standard v1.2
Report on Validation

Software Vendor Name:

Payment Software Name:

Date of Report:

Assessment End Date:

1 Contact Information and Report Summary

1.1 Contact Information

1.1.1 Assessed Software Vendor	
Specify the contact information for the assessed Software Vendor, including the Software Vendor's main point-of-contact for the Secure Software Assessment:	
Company name:	
DBA (doing business as):	
Mailing address:	
Company main website:	
Contact name:	
Contact title:	
Contact phone number:	
Contact email address:	

1.1.2 Secure Software Assessor Company	
Specify the contact information for Secure Software Assessor Company who performed the Secure Software Assessment:	
Company name:	
Mailing address:	
Company main website:	

1.1.3 Lead Assessor

Specify the contact information for Assessor responsible for the overall Secure Software Assessment, including their PCI credentials (Secure Software Assessor, Secure SLC Assessor, QSA, etc.):

Lead Assessor name:	
Lead Assessor phone number:	
Lead Assessor email address:	
Lead Assessor PCI credentials:	

1.1.4 Assessor Company Quality Assurance (QA) Reviewer

Identify the primary person responsible for conducting the required QA review for this Report on Validation (ROV):

QA reviewer name:	
QA reviewer phone number:	
QA reviewer email address:	
QA reviewer PCI credentials:	

1.1.5 Additional Assessors

Identify all other Assessor Company Employees involved in the Secure Software Assessment and their role/function during the assessment (adding rows as needed).

Assessor Name:	**Assessor PCI Credentials:**	**Assessor Role or Function During the Assessment:**

1.2 Additional Services Provided by Assessor Company

Section 2.2 of the *Qualification Requirements for SSF Assessors* specifies the independence requirements that the Assessor Company must adhere to at all times when conducting Secure Software Assessments. Assessors are encouraged to review the independence requirements prior to completing the following table:

1.2.1 Consultation Services Offered	
Indicate whether the Assessor Company provided the Software Vendor any consultation services on the implementation of controls to satisfy the control objectives and test requirements within the Secure Software Standard. If "yes," then describe the nature of the consultation.	
Confirmation of Consultation Services Provided:	**Description of Services Provided:**
☐ Yes ☐ No	

1.2.2 Other Products and Services Offered	
Disclose all other products or services provided by the Assessor Company to the Software Vendor that were reviewed during this assessment or that could reasonably be viewed to affect assessment independence (adding rows as needed).	
Product or Service Name:	**Product Description:**

1.2.3 Conflict of Interest Avoidance
Describe the efforts made to ensure that no conflict of interest resulted from the above-mentioned products and services provided by the Assessor Company.

1.3 Subcontracting

Indicate whether subcontracting was used at any point during the Secure Software Assessment and identify the SSF Assessor Company(s) involved, if applicable. Refer to Section 2.6 of the *Qualification Requirements for SSF Assessors* for more information on subcontracting.

1.3.1 Use of Subcontracting
Indicate whether any assessment activities were subcontracted to another SSF Assessor Company.
☐ Yes ☐ No

1.3.2 Subcontractors Used
Identify the SSF Assessor Company(s) used during the assessment.

2 Assessed Software

2.1 Software Name and Description

Describe the payment software assessed to the PCI Secure Software Standard:

2.1.1 Software Name and Listing Status			
Specify the software name and version(s) included in the assessment and indicate whether the assessed software is already listed on the PCI SSC List of Validated Payment Software. If already listed, then specify the Reference # (PCI Identifier) that corresponds to the listed payment software.			
Software name tested:		Software version(s) tested:	
Already listed on PCI SSC website?	☐ Yes ☐ No	PCI identifier (if applicable):	

2.1.2 Functional Details			
Identify which of the following Payment Software Types best represents the assessed payment software (select only one). Refer to Section A.2 of the *Secure Software Program Guide* for more information on Payment Software Types.			
☐ (01) POS Suite/General	☐ (04) Payment Back Office	☐ (07) POS Kiosk	☐ (10) Card-Not-Present
☐ (02) Payment Middleware	☐ (05) POS Admin	☐ (08) POS Face-to-Face/POI	☐ (11) Automated Fuel Dispenser
☐ (03) Payment Gateway/Switch	☐ (06) POS Specialized	☐ (09) Shopping Cart / Store Front	☐ (12) Payment Component
Describe the general software function and purpose (for example, the types of transactions performed, the payment acceptance channels supported, etc.).			

2.1.3 Architectural Details

Describe how the software is sold, distributed, or licensed to third parties (for example, as software-as-a-service, stand-alone application, component, etc.).
Describe a typical implementation of the software (for example, how it is configured in the execution environment, how it typically interacts with other components or services, where those components or services reside, and who is responsible for maintaining them).

<Insert payment software architecture diagram(s) here>

2.2 Software Versioning Methodology

Describe the versioning scheme used by the software vendor to identify and differentiate updates to the assessed payment software.

2.2.1 Version Format
Describe the format of the versioning scheme, such as number of elements, number of digits used for each element, format of separators used between elements and character set used for element (consisting of alphabetic, numeric, and/or alphanumeric characters).

2.2.2 Version Element Hierarchy
Describe the hierarchy of the elements, including what each element represents in the versioning scheme.

2.2.3 Additional Versioning Details
Specify any other important details regarding the versioning scheme used.

2.3 Required Dependencies

Identify any additional hardware, software, or services that must be implemented for the assessed software to function.

Required dependencies are those that would render the assessed payment software inoperable or useless, if unavailable. Such dependencies typically involve hardware, software or services that must be purchased, licensed, and/or maintained separately by an implementing entity (such as a merchant or other type of entity). These types of dependencies do not include hardware, software, or services that are packaged and distributed with the assessed software.

2.3.1 Hardware Dependencies

Does the assessed software require any specialized hardware device(s) for operation, such as a PCI-approved PTS device or other purpose-built device(s)?	☐ Yes ☐ No

If "Yes," then complete the following table (adding rows as needed). Each of the device attributes that must be specified are described below:

- **Provider / Supplier**: The manufacturer and/or supplier of the device. Also referred to as "device vendor."
- **Make / Model #**: The device name and/or model number.
- **Version(s) Supported**: The version(s) of the device that is/are supported by the assessed payment software.
- **Version(s) Tested**: The version(s) of the device that was/were used during the software assessment.
- **PTS Approval #**: The PTS approval number for the associated PCI-approved PTS device(s), where applicable. This information need only be specified if the required device(s) has been approved by PCI SSC under the PCI PIN Transaction Security (PTS) Point-of-Interaction (POI) device validation program.

Note 1: POI device approval listings that appear similar or identical on the PCI SSC List of Approved PTS Devices may be associated with different versions of the PTS POI Standard. Be sure the correct listing is referenced and used during the assessment. The most recent device approvals should be referenced.

Note 2: Ensure that the requisite requirements in the PCI Secure Software Standard are met and satisfied per POI Device Type included in the software assessment.

Provider / Supplier	**Make / Model #**	**Version(s) Supported**	**Version(s) Tested**	**PTS Approval #** (if applicable)

2.3.2 Software Dependencies

Does the assessed software require any specialized software for operation such as a particular operating system(s); database, application, or web server software; or a specific development framework like .Net or Java?	☐ Yes ☐ No

If "Yes," then complete the following table (adding rows as needed). Each of the device attributes that must be specified are described below:

- **Provider / Supplier**: The manufacturer and/or supplier of the software.
- **Software Name**: The name of the software.
- **Software Description**: A brief description of the software type and/or intended function (e.g., database, web server, etc.)
- **Version(s) Supported**: The version(s) of the software supported by the assessed payment software.
- **Version(s) Tested**: The version(s) of the software that was/were used during the software assessment.

Provider / Supplier	Software Name	Software Description	Version(s) Supported	Version(s) Tested

2.4 Sensitive Data

Identify the types of sensitive data stored, processed, or transmitted by the assessed software and describe how this data flows through the software.

2.4.1 Sensitive Data Overview

Identify the data stored, processed, or transmitted by the software that requires confidentiality and/or integrity protection, and the locations where this information is stored persistently (if applicable).

- **Sensitive Data Type**: The type of data deemed sensitive. Examples include Account Data, authentication credentials, cryptographic keys, etc.
- **Sensitive Data Elements**: The names of the individual data elements in relation to the Sensitive Data Type. Examples include PAN/SAD, username/password, etc.
- **Protection Requirements**: Indicates whether the data requirements confidentiality or integrity protection, or both.
- **Storage Locations**: The locations where sensitive data is stored persistently. Examples include file [name], table [name], etc.

Sensitive Data Type	Sensitive Data Elements	Protection Requirements	Storage Location(s)

2.4.2 Sensitive Data Flows

Provide high-level data flow diagrams that show the details of all sensitive data flows, including:

- All flows and locations of encrypted sensitive data (including all sensitive data inputs/outputs both within and outside the execution environment).
- All flows and locations of clear-text sensitive data (including all sensitive data inputs/outputs both within and outside the execution environment).

For each data flow, identify the following:

- How and where sensitive data is stored, processed and/or transmitted.
- The specific types and details of the sensitive data involved (e.g., full track, PAN, PIN, expiry date, user IDs, passwords, etc.)
- All components involved in the storage, processing, or transmission of sensitive data.
- All sensitive functions and resources associated with the sensitive data flow.

Note: Specify all types of sensitive data flows, including any output to hardcopy, paper, or other external media. Sensitive data flows must also denote locations where sensitive data crosses trust boundaries and where it is passed to other applications or services that were not included in the assessment.

Insert a narrative response here to address the reporting instructions the diagrams below do not adequately address:

<Insert data flow diagram(s) here>

3 Assessment Overview

3.1 Assessment Date

3.1.1 ROV Completion Date	
Specify the date the ROV was completed. This date is the same as the "ROV Completion Date" in the Secure Software AOV and represents the date the Assessor Company and Software Vendor agreed on the final version of the ROV.	
ROV completion date:	

3.1.2 Assessment Start Date	
Specify the date the assessment began. This is the first date that evidence was gathered, or observations were made.	
Assessment start date:	

3.1.3 Assessment End Date	
Specify the date the assessment ended. This is the last date that evidence was gathered, or observations were made.	
Assessment end date:	

3.1.4 PCI Secure Software Standard Version	
Specify the version of the PCI Secure Software Standard used for this assessment.	
Version used:	

3.2 Assessment Scope

3.2.1 Assessed Requirement Modules

Identify the requirement modules within the *PCI Secure Software Standard* to which the payment software was assessed and provide justification for why other modules were not included in the assessment.

Assessed Modules		Justification (if excluded from the software assessment)
☐	Core Requirements	N/A
☐	Module A – Account Data Protection Requirements	
☐	Module B – Terminal Software Requirements	
☐	Module C – Web Software Requirements	

3.2.2 Requirements Deemed Not Applicable

Identify any control objectives and test requirements that were determined to be "Not Applicable" to the assessed software or the assessed software vendor. List applicable control objectives and test requirements in the order they appear in Section 4, "Detailed Findings and Observations" (adding additional rows as needed).

Important Note: A "Not Applicable" finding is only acceptable where the control objective has been verified to be not applicable to the assessed software through an appropriate degree of testing. All "Not Applicable" responses MUST be tested, and details MUST be provided to describe how it was determined that a control objective does not apply to the assessed software.

Control Objective or Test Requirement #:	Describe how it was determined that the requirement is Not Applicable to the assessed software:

3.3 Assessor Evidence

3.3.1 Documentation and Evidence Obtained

Identify and list all of the documents, materials, and other evidence obtained and reviewed during the assessment. Additional rows may be added as needed. The required attributes that must be specified for each document are described below:

- **Reference #**: A reference number used to uniquely identify the documentation or evidence obtained during the assessment. Generic values, such as "Doc-1," "Doc-2," and so on, may be used in lieu of formal reference numbers.
- **Document Name**: The title given to the documentation or evidence obtained. Document Names may be formal or informal and should include any relevant version information (if applicable).
- **Document Description / Purpose**: A brief description of the contents and/or purpose of the documentation or evidence obtained.
- **Date Created**: The date the documentation or evidence was last generated or updated.
- **Date Reviewed**: The date the documentation or evidence was last retrieved. In certain cases, the Date Reviewed may be the same as the Date Created (for example, where the documentation or evidence is generated by the Assessor during testing).
- **Source**: The entity who created and/or generated the documentation or evidence. Documentation and evidence are typically the responsibility of the Software Vendor or a third-party to create and maintain. However, it may be necessary for the Assessor to generate their own evidence to verify compliance with a particular Secure Software Requirement. Acceptable values for this field are "Vendor," "Assessor," or "Third-Party."

Reference #	Document Name	Document Description / Purpose	Date Created	Date Reviewed	Source

3.3.2 Individuals Interviewed

Identify and list the individuals interviewed during the assessment. Additional rows may be added as needed. The required attributes that must be specified for each interviewee are described below:

- **Reference #**: A reference number used to uniquely identify each distinct interview. Generic values such as "Int-1," "Int-2," and so on may be used in lieu of formal reference numbers.
- **Interviewee(s)**: The name of the individual(s) who participated in the interviews.
- **Job Title**: The job title or job function of the interviewee(s).
- **Organization**: The organization(s) represented by the interviewee(s).
- **Topics Covered**: A high-level summary of the topics covered during each interview.
- **Interview Notes Ref#**: The notes and/or audio files generated by the Assessor to record the interview results. Values in this column should include references to the appropriate documentation or evidence recorded in Section 3.3.1, "Documentation and Evidence Obtained."

Reference #	Interviewee(s)	Job Title	Organization	Topics Covered	Interview Notes Ref#

3.3.3 Software Testing Performed

Identify and describe the software testing performed during the assessment and the scope of each test. Additional rows may be added as needed.

Tests may be grouped together if performed as part of a common test goal or objective. However, the details provided in each row should be sufficient to differentiate tests where variations are necessary to validate different Secure Software Requirements.

The required attributes that must be specified for each test are described below:

- **Reference #**: A reference number used to uniquely identify each distinct test. Generic values such as "Test-1," "Test-2," and so on may be used in lieu of formal reference numbers.
- **Test Description**: A brief description of the types of testing performed (static source code analysis, dynamic analysis), the tools or methods used, etc.
- **Test Scope**: The specific features, functions, or components assessed. Examples could include module names (user authentication module, payment module, etc.), webpages (transaction summary page, payment page), etc.
- **Test Objective / Purpose**: The primary purpose of the test(s). Example objectives include "determining how the payment software responds to brute force password attempts" or "detecting vulnerabilities on payment pages."

Reference #	Test Description	Test Scope	Test Objective / Purpose

3.4 Sampling

3.4.1 Sampling Methodology

Did the Assessor use sampling to validate any Secure Software Requirements?	☐ Yes ☐ No

If "Yes," then summarize the assessor's sampling methodology, including how the assessor determines sample size and any minimum sample sizes used. Also include any additional factors that contribute to determining an appropriate sample size (total population, risk, frequency with which the security control is performed, number of deviations expected, etc.).

3.4.2 Sample Sets Used

If "Yes," then identify all the sample sets used during the assessment (adding rows as needed).

Where sampling is used, samples must be representative of the total population of possible items. The sample size must be sufficiently large and diverse to provide assurance that the selected sample accurately reflects the overall population.

The required attributes that must be specified for each sample set are described below:

- **Reference #**: A reference number used to uniquely identify each sample set. Generic values such as "Set-1," "Set-2," and so on may be used in lieu of formal reference numbers.
- **Sample Description**: A brief description of the items sampled. For example, "a sample of software updates" or "a sample of user IDs."
- **Total Sampled**: The number of items included in the sample set. This could also be expressed in other relevant terms, such as lines of code (if applicable).
- **Total Population**: The total number of possible items available for testing.
- **Sample Justification**: The Assessor's justification for why the Total Sampled is a fair and accurate representation of the Total Population of potential items available for sampling.

Reference #	Sample Description	Total Sampled	Total Population	Sample Justification

3.5 Summary of Findings

Describe the results of the overall Secure Software Assessment and for each principal control objective.

3.5.1 Overall Assessment Result	
The Assessor must confirm each of the following prior to submitting this ROV to PCI SSC:	
☐	**Validated**: All applicable control objectives are marked "In Place," thereby *Secure Software Name(s) and Version(s)* has achieved full validation with the PCI Secure Software Standard.
☐	The ROV was completed according to the PCI Secure Software Standard Version 1.2, in adherence with the instructions therein.
☐	All information within this ROV represents this Secure Software Assessment in all material aspects.

3.5.2 Additional Findings or Information (Optional)
This optional field is provided for the Assessor to document any additional information or context regarding the assessed payment software that would help PCI SSC to better understand the findings documented in this ROV.

3.6 Assessor Attestation and Signature

Upon completion of a Secure Software Assessment, the Lead Assessor must confirm each of the following and **sign in Section 3.6.5 below**. This entire section must be printed and signed manually, or digitally signed using a PCI SSC-accepted electronic/digital signature.

3.6.1	Attestation of Independence
☐	This assessment was conducted strictly in accordance with all applicable requirements set forth in Section 2.2 of the Qualification Requirements for SSF Assessors, including but not limited to the requirements therein regarding independence, independent judgment and objectivity, disclosure, conflicts of interest, misrepresentations, and instruction of employees.
☐	This assessment was conducted in a manner intended to preserve at all times the professional judgment, integrity, impartiality, and professional skepticism of the SSF Assessor Company.
☐	This Report on Validation accurately identifies, describes, represents, and characterizes all factual evidence that the SSF Assessor Company and its Assessor Employees gathered, generated, discovered, reviewed and/or determined in their sole discretion to be relevant to this assessment while performing the assessment.
☐	The judgments, conclusions, and findings contained in this Report on Validation (a) accurately reflect and are based solely upon the factual evidence described immediately above, (b) reflect the independent judgments, findings and conclusions of the SSF Assessor Company and its Assessor Employees only, acting in their sole discretion, and (c) were not in any manner influenced, directed, controlled, modified, provided or subjected to any prior approval by the assessed Vendor, any contractor, representative, professional advisor, agent or affiliate thereof, or any other person or entity other than the SSF Assessor Company and its Assessor Employees.

3.6.2	Attestation of Software Eligibility
☐	To the best of my knowledge, the assessed payment software is eligible for validation in accordance with the *Secure Software Program Guide*.

3.6.3	Attestation of Scoping Accuracy
☐	To the best of my knowledge, all information pertaining to the scope of the Secure Software Assessment is accurately represented in Section 3.2, “Assessment Scope” of this Report on Validation.

3.6.4	Attestation of Sampling
☐	To the best of my knowledge, all sample sets used for this Secure Software Assessment are accurately represented in Section 3.4.2, “Sample Sets Used” of this Report on Validation.

3.6.5 Lead Assessor Signature	
Signature of Lead Assessor:	*Date:*
Lead Assessor Name:	*SSF Assessor Company Name:*

4 Detailed Findings and Observations

Complete this section by identifying whether each control objective is “In Place,” “Not in Place,” or “N/A” (Not Applicable) and describe the detailed findings and observations for each of the associated test requirements.

4.1 Core Module

Control Objectives / Test Requirements	Reporting Instructions	Assessor’s Findings		
Control Objective 1: Critical Asset Identification All software critical assets are identified.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
1.1 All sensitive data stored, processed, or transmitted by the software is identified.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
1.1.a The assessor shall examine evidence to confirm that information is maintained that details all sensitive data that is stored, processed, and/or transmitted by the software. At a minimum, this shall include all payment data; authentication credentials; cryptographic keys and related data (such as IVs and seed data for random number generators); and system configuration data (such as registry entries, platform environment variables, prompts for plaintext data in software allowing for the entry of PIN data, or configuration scripts).	**R1** Identify the evidence obtained that details the sensitive data that is stored, processed, and transmitted by the assessed software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
1.1.b The assessor shall examine evidence to confirm that information is maintained that describes where sensitive data is stored. This includes the storage of sensitive data in temporary storage (such as volatile memory), semi-permanent storage (such as RAM disks), non-volatile storage (such as magnetic and flash storage media), or in specific locations or form factors (such as with an embedded system that is only capable of local storage).	**R1** Identify the evidence obtained that details the locations where sensitive data is stored.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
1.1.c The assessor shall examine evidence to confirm that information is maintained that describes the security controls that are implemented to protect sensitive data.	**R1** Identify the evidence obtained that details the security controls that are implemented to protect sensitive data during storage, processing, and transmission.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
1.1.d The assessor shall test the software to validate the evidence obtained in Test Requirements 1.1.a through 1.1.c.	**R1** Describe each of the tests performed, including the tool(s) and/or method(s) used, to confirm that the evidence obtained in Test Requirement 1.1.a accurately reflects the sensitive data stored, processed, and transmitted by the assessed software.	
	R2 Describe each of the software tests performed, including the tool(s) and/or method(s) used and the scope of each test, to confirm that the evidence obtained in Test Requirement 1.1.b accurately reflects the locations where sensitive data is stored.	
	R3 Describe each of the software tests performed, including the tool(s) and/or method(s) used and the scope of each test, to confirm that the evidence obtained in Test Requirement 1.1.c accurately reflects the software security controls implemented to protect sensitive data.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	
1.1.e The assessor shall examine evidence and test the software to identify the transaction types and/or card data elements that are supported by the software, and to confirm that the data for all of these is supported by the evidence examined in Test Requirements 1.1.a through 1.1.c.	**R1** Identify the evidence obtained that details the transaction types supported, and the associated card data elements stored, processed, and transmitted by the assessed software.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
1.1.f The assessor shall examine evidence and test the software to identify the cryptographic implementations that are supported by the software (including cryptography used for storage, transport, and authentication), and to confirm that the cryptographic data for all of these implementations is supported by the evidence examined in Test Requirements 1.1.a through 1.1.c, and that the evidence describes whether these are implemented by the software itself, through third-party software, or as functions of the execution environment.	**R1** Identify the evidence obtained that details the cryptographic implementations supported by the assessed software and whether they are implemented by the software itself, through third-party software, or as functions of the execution environment.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
1.1.g The assessor shall examine evidence and test the software to identify the accounts and authentication credentials supported by the software (including both default and user-created accounts) and to confirm that these accounts and credentials are supported by the evidence examined in Test Requirements 1.1.a through 1.1.c.	**R1** Identify the evidence obtained that details the types of authentication methods and credentials supported by the assessed software.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
1.1.h The assessor shall examine evidence and test the software to identify the configuration options provided by the software that can impact sensitive data (including those provided through separate files or scripts, internal functions, or menus and options), and to confirm that these are supported by the evidence examined in Test Requirements 1.1.a through 1.1.c.	**R1** Identify the evidence obtained that details the configuration options provided by the assessed software that can impact the security of sensitive data.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
1.2 All sensitive functions and sensitive resources provided or used by the software are identified.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
1.2.a The assessor shall examine evidence to confirm that information is maintained that details all sensitive functions and sensitive resources provided or used by the software. At a minimum, this shall include all functions that are designed to store, process, or transmit sensitive data and those services, configuration files, or other information necessary for the normal and secure operation of those functions.	**R1** Identify the evidence obtained that details the sensitive functions and sensitive resources provided or relied upon by the assessed software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
1.2.b The assessor shall examine evidence to confirm that information is maintained that clearly describes how and where the sensitive data associated with these functions and resources is stored. This includes the storage of sensitive data in temporary storage (such as volatile memory), semi-permanent storage (such as RAM disks), and non-volatile storage (such as magnetic and flash storage media). The assessor shall confirm that this information is supported by the evidence examined in Test Requirement 1.1.a through 1.1.c.	**R1** Identify the evidence obtained that details the locations where sensitive data that is associated with sensitive functions and sensitive resources are stored.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
1.2.c Where the sensitive functions or sensitive resources are provided by third-party software or systems, the assessor shall examine evidence and test the software to confirm that the software correctly follows available guidance for the third-party software. ***Note**: For example, by reviewing the security policy of a PTS or FIPS140-2 or 140-3 approved cryptographic system.*	**R1** Indicate whether the assessed software relies upon any sensitive functions or sensitive resources during operation that are provided by third-party software or systems.	☐ Yes ☐ No		
	R2 If R1 is "No," then describe what the assessor observed in the evidence obtained that confirms the software does not rely upon any sensitive functions or sensitive resources during software operation that are provided by third-party software or systems.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
	R3 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms the assessed software implements the third-party software or systems in accordance with third-party software vendor guidance.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			
1.3 Critical assets are classified.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
1.3 The assessor shall examine evidence to confirm that: • The software vendor defines criteria for classifying critical assets in accordance with the confidentiality, integrity, and resiliency requirements for each critical asset. • An inventor of all critical assets with appropriate classifications is maintained.	**R1** Identify the evidence obtained that details the confidentiality, integrity, and resiliency requirements for each critical asset.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 2: Secure Defaults Default privileges, features, and functionality are restricted to only those necessary to provide a secure default configuration.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
2.1 All functions exposed by the software are enabled by default only when and where it is a documented and justified part of the software architecture.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
2.1.a The assessor shall examine evidence and test the software to identify any software APIs or other interfaces that are provided or exposed by default upon installation, initialization, or first use. For each of these interfaces, the assessor shall confirm that the vendor has documented and justified its use as part of the software architecture. Testing shall include methods to reveal any exposed interfaces or other software functionality (such as scanning for listening services where applicable). ***Note**: This includes functions that are auto-enabled as required during operation of the software.*	**R1** Identify the evidence obtained that details all interfaces (user interfaces, APIs, etc.) that are accessible or that can be made accessible (through user input or interaction) upon software installation, initialization, or first use.			
	R2 Describe what the assessor observed in the evidence obtained that confirms that all accessible interfaces are reflected in the software vendor's documentation.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
2.1.b The assessor shall test the software to determine whether any of the interfaces identified in Test Requirement 2.1.a rely on external resources for authentication. Where such resources are relied upon, the assessor shall examine evidence to confirm that methods are implemented to ensure that proper authentication remains in place and that these methods are included in the assessment of other applicable requirements in this standard.	**R1** Indicate whether any of the interfaces identified in Test Requirement 2.1.a rely on external resources for authentication, such as those that are provided by the execution environment or that reside outside of the execution environment.	☐ Yes ☐ No		
	R2 If R1 is "No," then describe what the assessor observed that confirms that none of the interfaces identified in Test Requirement 2.1.a rely on external resources for authentication.			
	R3 If R1 is "Yes," then describe the methods that are implemented to ensure that proper authentication always remains in place during software operation.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	
2.1.c The assessor shall test the software to determine whether any of the interfaces identified in Test Requirement 2.1.a rely on external resources for the protection of sensitive data during transmission. Where such resources are relied upon, the assessor shall examine evidence to confirm that methods are implemented to ensure proper protection remains in place and that these methods are included in the assessment of other applicable requirements in this standard.	**R1** Indicate whether any of the interfaces identified in Test Requirement 2.1.a rely on external resources for the protection of sensitive data.	☐ Yes ☐ No
	R2 If R1 is "No," then describe what the assessor observed that confirms that none of the interfaces identified in Test Requirement 2.1.a rely on external resources for the protection of sensitive data.	
	R3 If R1 is "Yes," then describe the methods that are implemented to ensure that the protection of sensitive data always remains in place during software operation.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	
2.1.d The assessor shall test the software to determine whether any of the interfaces identified in Test Requirement 2.1.a expose functions or services that have publicly disclosed vulnerabilities by conducting a search on the exposed protocols, methods, or services in public vulnerability repositories such as that maintained within the National Vulnerability Database.	**R1** Indicate whether any of the interfaces identified in Test Requirement 2.1.a rely on any protocols, functions, or ports that are known to contain vulnerabilities.	☐ Yes ☐ No
	R2 If R1 is "No," then describe what the assessor observed that confirms the software does not use or otherwise rely on known vulnerable protocols, functions, or ports.	
	R3 If R1 is "Yes," then identify the protocols, functions, or ports known to contain vulnerabilities.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
2.1.e Where known vulnerabilities in exposed interfaces exist, the assessor shall examine evidence and test the software to confirm the following: • Methods are implemented to mitigate the exploitation of these weaknesses. • The risks posed by the use of known vulnerable protocols, functions, or ports are documented. • Clear and sufficient guidance on how to correctly implement sufficient security to meet applicable control objectives in this standard is provided to stakeholders in accordance with Control Objective 12.1. ***Note**: The assessor should reference the vendor threat information defined in Control Objective 4.1 for this item.*	**R1** Identify the evidence obtained that details the software vendor's analysis of the risks of using known vulnerable protocols, functions, and ports.	
	R2 Describe the protection methods that are implemented to mitigate the exploitation of known vulnerable protocols, functions, and ports.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
2.1.f The assessor shall examine evidence to identify any third-party modules used by the software and to confirm that any such functions exposed by each module are disabled, unable to be accessed through mitigation methods implemented by the software, or formally documented and justified by the software vendor. Where access to third-party functions is prevented through implemented protection methods, the assessor shall test the software to confirm that it does not rely on a lack of knowledge of such functions as a security mitigation method by simply not documenting an otherwise accessible API interface, and to confirm that the protection methods are effective at preventing the insecure use of such third-party functions.	**R1** Indicate whether the software exposes or otherwise facilitates access to any functions provided by third-party modules upon software installation, initialization, or first use.	☐ Yes ☐ No
	R2 If R1 is "No," then describe what the assessor observed that confirms the software does not facilitate access to any such functions upon software installation, initialization, or first use.	
	R3 If R1 is "Yes," then describe the methods implemented to prevent the insecure use of such third-party functions.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
2.2 All software security controls, features, and functions are enabled upon software installation, initialization, or first use. ***Note**: Specific software security controls required to protect the integrity and confidentiality of sensitive data, sensitive functions, and sensitive resources are captured in the Software Protection Mechanisms section.*		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
2.2.a The assessor shall examine evidence and test the software to identify all software security controls, features and functions relied upon by the software for the protection of critical assets and to confirm that all are enabled upon installation, initialization, or first use of the software.	**R1** Identify the evidence obtained that details the software security controls, features, and functions relied upon by the software for the protection of critical assets.			
	R2 Describe what the assessor observed that confirms that all software security controls, features, and functions relied upon by the software for the protection of critical assets are enabled (or can be enabled) upon software installation, initialization, or first use.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
2.2.b Where any software security controls, features and functions are enabled only upon initialization or first use, the assessor shall test the software to confirm that sensitive data is processed only after this initialization process is complete.	**R1** Indicate whether any software security controls relied upon by the software for the protection of critical assets can only be enabled upon software initialization or first use.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the methods implemented to ensure that payment data is not processed until the initialization process is complete.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
2.2.c Where user input or interaction is required to enable software security controls, features, or functions (such as the installation of certificates), the assessor shall examine evidence to confirm that clear and sufficient guidance on configuring these options is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether user input or interaction is required to enable any software security controls, features, or functions after installation, initialization, or first use.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance for configuring all configurable software security controls, features, or functions.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
2.3 Default authentication credentials or keys for built-in accounts are not used after software installation, initialization, or first use.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
2.3.a The assessor shall examine evidence to identify the default credentials, keys, certificates, and other critical assets used for authentication by the software. ***Note**: The assessor should refer to evidence obtained in the testing of Control Objectives 1, 5, and 7 to determine the authentication and access control mechanisms, keys, and other critical assets used for authentication.*	**R1** Identify the evidence obtained that details the credentials, keys, certificates, and other data relied upon by the software for authentication purposes.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
2.3.b The assessor shall test the software to confirm that all default credentials, keys, certificates, and other critical assets used for authentication by the software are supported by the evidence examined. ***Note**: It is expected that this analysis will include, but not necessarily be limited to, the use of entropy analysis tools to look for hardcoded cryptographic keys, searches for common cryptographic function call and structures such as S-Boxes and big-number library functions (and tracing these functions backwards to search for hardcoded keys), as well as checking for strings containing common user account names or password values.*	**R1** Describe the tests performed, including the tool(s) and/or method(s) used and the scope of each test, to confirm that the evidence obtained in Test Requirement 2.3.a accurately represents the credentials, keys, certificates, and other data relied upon by the software for authentication purposes.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
2.3.c Where user input or interaction is required to disable or change any authentication credentials or keys for built-in accounts, the assessor shall examine evidence to confirm that guidance on configuring these options is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether user input or interaction is required to disable or change default authentication credentials for built-in accounts.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to change or disable default authentication credentials for built-in accounts after software installation, initialization, or first use.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
2.3.d The assessor shall test the software to confirm that default authentication credentials or keys for built-in accounts are not used by the authentication and access control mechanisms implemented by the software after software installation, initialization, or first use. ***Note**: The assessor should refer to evidence obtained in the testing of Control Objective 5 to determine the authentication and access control mechanisms implemented by the software.*	**R1** Describe the tests performed, including the tool(s) and/or method(s) used and the scope of each test, to confirm that default credentials and keys for built-in accounts are not used by the software after installation, initialization, or first use.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
2.3.e The assessor shall test the software to confirm that cryptographic keys used for authentication are not used for other purposes, such as protecting sensitive data during storage and transmission. ***Note**: The assessor should refer to evidence obtained in the testing of Control Objective 6 to determine the software security controls implemented to protect sensitive data.*	**R1** Identify the evidence obtained that details the purposes for which cryptographic keys are used by the software.			
	R2 Describe what the assessor observed that confirms that cryptographic keys used for authentication are not also used for other purposes.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
2.4 The privileges and resources requested by the software from its execution environment are limited to those necessary for the operation of the software.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
2.4.a The assessor shall examine evidence to identify the privileges and resources required by the software and to confirm that information is maintained that describes and reasonably justifies all privileges and resources required, including explicit permissions for access to resources, such as cameras, contacts, etc.	**R1** Identify the evidence obtained that details the resources and access privileges required by the software from the execution environment, and the software vendor's justification for why such resources and access privileges are necessary.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
2.4.b Where limiting access is not possible due to the architecture of the solution or the execution environment in which the software is executed, the assessor shall examine evidence to identify all mechanisms implemented by the software to prevent unauthorized access, exposure, or modification of critical assets, and to confirm that guidance on properly implementing and configuring these mechanisms is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software requires "admin" or other elevated privileges to any functions or resources within the execution environment.	☐ Yes ☐ No		
	R2 If R1 is "No," then describe what the assessor observed in the evidence obtained that confirms the software does not require "admin" or other elevated privileges to functions or resources within the execution environment.			
	R3 If R1 is "Yes," then describe the methods or mechanisms implemented to prevent unauthorized users from using the privileges to access, expose, or modify critical assets.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
	R4 If R1 is "Yes," identify the evidence obtained that contains the software vendor's guidance on how to implement and configure such protection methods or mechanisms.	
	R5 Describe any other assessment activities and/or findings for this test requirement.	
2.4.c The assessor shall test the software to confirm that access permissions and privileges are assigned according to the evidence examined in Test Requirement 2.4.a. The assessor shall, where possible, use suitable tools for the platform on which the software is installed to review the permissions and privileges of the software itself, as well as the permissions and privileges of any resources, files, or additional elements generated or loaded by the software during use. ***Note**: Where the above testing is not possible, the assessor shall justify why this is the case and that the testing that has been performed is sufficient.*	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to verify that the evidence obtained in Test Requirement 2.4.a accurately reflects the execution environment resources and access privileges required by the assessed software.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
2.4.d Where the software execution environment provides legacy features for use by older versions of the software, the assessor shall examine evidence and test the software to confirm that these are not used, and that only recent and secured functionality is implemented. For example, software should "target" the latest versions of APIs provided by the environment on which they run, where available.	**R1** Indicate whether the software relies on any legacy APIs, functions, or features provided by the execution environment.	☐ Yes ☐ No
	R2 If R1 is "No," then describe what the assessor observed that confirms that such features are not relied upon.	
	R3 If R1 is "Yes," then describe the protection methods implemented to secure the use of legacy features.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
2.5 Default privileges for built-in accounts are limited to those necessary for their intended purpose or function.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
2.5.a The assessor shall examine evidence to identify all default accounts provided by the software and to confirm that the privileges assigned to these accounts are justified and reasonable.	**R1** Identify the evidence obtained that details the default privileges assigned to built-in accounts and the software vendor's justification for assigning such privileges by default.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
2.5.b The assessor shall test the software to confirm that all default accounts provided or used by the software are supported by the evidence examined in Test Requirement 2.5.a.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to verify that the evidence obtained in Test Requirement 2.5.a accurately reflects the built-in accounts and default privileges assigned to those accounts.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
2.5.c The assessor shall examine evidence and test the software to confirm that exposed interfaces, such as APIs, are protected from attempts by unauthorized users to modify account privileges and elevate user access rights.	**R1** Describe the methods implemented to protect the interfaces identified in Test Requirement 2.1.a from attempts by unauthorized users to modify access privileges.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 3: Sensitive Data Retention Retention of sensitive data is minimized.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
3.1 The software only retains the sensitive data absolutely necessary for the software to provide its intended functionality.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
3.1.a The assessor shall examine evidence to identify the sensitive data that is collected by the software for use beyond any one transaction, the default time period for which it is retained, and whether the retention period is user-configurable, and to confirm that the purpose for retaining the sensitive data in this manner is justified and reasonable. ***Note**: The assessor should refer to evidence obtained in the testing of Control Objective 1.1 to determine the sensitive data retained by the software.*	**R1** Identify the evidence obtained that details the sensitive data collected and retained by the software beyond a single transaction, the default time period for which it is retained, and whether the retention period is user configurable.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
3.1.b The assessor shall test the software to confirm that all available functions or services designed for the retention of sensitive data are supported by the evidence examined in Test Requirement 3.1.a. ***Note**: The assessor should refer to evidence obtained in the testing of Control Objective 1.2 to determine the sensitive functions and services provided or used by the software.*	**R1** Describe the tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that the sensitive data identified in Test Requirement 3.1.a accurately reflects the sensitive data retained persistently by the software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
3.1.c The assessor shall examine evidence and test the software to determine whether the software facilitates the storage of persistent sensitive data for the purposes of debugging, error finding or testing of systems, and to confirm that such data is protected during storage in accordance with Control Objective 6.1. Any function that allows for the storage of sensitive data for these purposes must be explicitly enabled through an interface that requires interaction and authorization by the user and retains the data only for the duration necessary in accordance with reasonable vendor criteria. Closure of the software must result in termination of this debugging state, such that it requires explicit re-enablement when the software is next executed, and any sensitive data is securely deleted per Control Objective 3.4.	**R1** Indicate whether the software facilitates the persistent storage of sensitive data for the purposes of debugging, error finding, or system testing.	☐ Yes ☐ No
	R2 If R1 is "No," then describe what the assessor observed that confirms that sensitive data is not retained persistently for this purpose.	
	R3 If R1 is "Yes," then describe the methods implemented to protect sensitive data when retained for this purpose.	
	R4 If R1 is "Yes," then describe how the software handles sensitive data retained for this purpose when debugging, error finding, and/or testing functions are terminated.	
	R5 Describe any other assessment activities performed and/or findings for this test requirement.	
3.1.d Where user input or interaction is required to configure the retention period of sensitive data, the assessor shall examine vendor evidence to confirm that there is clear and sufficient guidance on this process provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**R1** Indicate whether the software requires or otherwise enables users to configure the retention period for persistently stored sensitive data.	☐ Yes ☐ No
	R2 If R1 is "Yes," identify the evidence obtained that details the options available to users to configure the retention periods for this data.	
	R3 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring available options.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
3.2 Transient sensitive data is retained only for the duration necessary to fulfill a legitimate business purpose.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
3.2.a Using information obtained in Test Requirement 1.1.a, the assessor shall examine evidence to identify all sensitive data that is retained by the software for transient use, what triggers the secure deletion of this data, and to confirm that the purposes for retaining the data are justified and reasonable. This includes data that is stored only in memory during the operation of the software.	**R1** Identify the evidence obtained that details the sensitive data that is retained by the software for transient use.			
	R2 Describe the mechanisms used or relied upon by the software to securely delete sensitive data from transient storage facilities once the purpose for retaining this data has been fulfilled.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
3.2.b Using information obtained in Test Requirement 1.2.a, the assessor shall test the software to confirm that all available functions or services that retain transient sensitive data are supported by evidence examined in Test Requirement 3.2.a and do not use immutable objects.	**R1** Indicate whether any sensitive data identified in Test Requirement 3.2.a is stored using immutable objects.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the constraints that exist that require or otherwise necessitate the use of immutable objects.			
	R3 If R1 is "Yes," then describe the protection mechanisms implemented to mitigate the risks posed by the use of immutable objects.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
3.2.c The assessor shall examine evidence and test the software to determine whether the software facilitates the storage of transient sensitive data for the purposes of debugging, error finding or testing of systems, and to confirm that such data is protected in accordance with Control Objective 6.1. Any function that allows for the storage of transient sensitive data for these purposes must be explicitly enabled through an interface that requires interaction and authorization by the user. Closure of the software must result in the termination of this debugging state, such that it requires explicit re-enablement when the software is next executed, and any transient sensitive data is securely deleted in accordance with Control Objective 3.5.	**R1** Indicate whether the software facilitates the storage of sensitive data in temporary storage facilities for the purposes of debugging, error finding, or system testing.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe the methods implemented to protect this data when retained for this purpose.	
	R3 If R1 is "Yes," then describe how the software handles this data when debugging, error finding, and/or testing functions are terminated.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	
3.2.d Where users can configure retention of transient sensitive data, the assessor shall examine vendor evidence to confirm that clear and sufficient guidance on this process is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**R1** Indicate whether the software requires or otherwise enables users to configure the retention periods for sensitive data stored in temporary storage facilities.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the options available to users to configure the retention periods for this data.	
	R3 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring available options.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

3.3 The software protects the confidentiality and integrity of sensitive data (both transient and persistent) during retention. ***Note**: The Software Protection Mechanisms section includes several specific software security controls that are required to be implemented to protect sensitive data during storage, processing, or transmission. Those software security controls should be analyzed to determine their applicability to the types of sensitive data retained by the software.*	**In Place**	**Not in Place**	**N/A**
	☐	☐	☐

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
3.3.a The assessor shall examine the evidence to identify the methods implemented to protect sensitive data during storage.	**R1** Identify the evidence examined that details the methods implemented and/or relied upon to protect sensitive data (both transient and persistent) during retention.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
3.3.b Where sensitive data is stored outside of temporary variables within the code itself, the assessor shall test the software to confirm that sensitive data is protected using either strong cryptography or other methods that provide an equivalent level of security.	**R1** Indicate whether the software stores any sensitive data within the code itself (e.g., is 'hardcoded').	☐ Yes ☐ No
	R2 If R1 is "No," describe how the assessor confirmed that no sensitive data is stored within the code.	
	R3 If R1 is "Yes," then identify the evidence obtained that details the locations within the code where this data is stored.	
	R4 If R1 is "Yes," then describe the methods implemented to protect this data from unauthorized disclosure and/or modification (as applicable).	
	R5 Describe any other assessment activities performed and/or findings for this test requirement.	
3.3.c Where protection methods use cryptography, the assessor shall examine evidence and test the software to confirm that the cryptographic implementation complies with Control Objective 7 of this standard.	**R1** Indicate whether the software uses or relies on cryptography for the protection of stored sensitive data (transient or persistent).	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the cryptographic algorithms and modes of operation used or relied upon by the software.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
3.3.d Where sensitive data is protected using methods other than strong cryptography, the assessor shall examine evidence and test the software to confirm that the protections are present in all environments where the software is designed to be executed and are implemented correctly	**R1** Indicate whether any methods other than strong cryptography are used or relied upon by the software for the protection of stored sensitive data (transient or persistent).	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe the protection methods used or relied upon by the software for this purpose.	
	R3 If R1 is "Yes," then describe the methods implemented to ensure that these protection methods are present in all environments where the software is designed to be executed.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	
3.3.e Where user input or interaction is required to configure protection methods, the assessor shall examine evidence to confirm that guidance on configuring these options is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software requires or otherwise enables users to configure methods to protect sensitive data in storage facilities (transient or persistent).	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the options available to users for configuring protection methods.	
	R3 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring available options.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
3.4 The software securely deletes persistent sensitive data when no longer needed.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
3.4.a The assessor shall examine evidence to identify the methods implemented to render persistent sensitive data irretrievable and to confirm that sensitive data is rendered unrecoverable after the process is complete.	**R1** Identify the evidence obtained that details the methods implemented to render persistent sensitive data irretrievable when no longer needed.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
3.4.b The assessor shall examine evidence and test the software to identify any platform or implementation level issues that complicate the secure deletion of non-transient sensitive data and to confirm that any non-transient sensitive data is securely deleted using a method that ensures that the data is rendered unrecoverable. Methods may include (but are not necessarily limited to) overwriting the data, deletion of cryptographic keys (of sufficient strength) that have been used to encrypt the data, or platform-specific functions that provide for secure deletion. Methods must accommodate for platform-specific issues, such as flash wear-levelling algorithms or SSD over-provisioning, which may complicate simple over-writing methods.	**R1** Indicate whether known platform or implementation-level issues exist that complicate the secure deletion of sensitive data from persistent data stores.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the methods implemented to mitigate the risks associated with such complications.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
3.4.c The assessor shall test the software using forensic tools to identify any non-transient sensitive data residue in the execution environment, and to confirm that the methods attested by the software vendor are correctly implemented and applied to all sensitive data. This analysis should accommodate for the data structures and methods used to store the sensitive data (for example, by examining file systems at the allocation level and translating data formats to identify sensitive data elements) and cover all non-transient sensitive data types. ***Note:*** *Where forensic testing of some or all aspects of the platform is not possible, the assessor should examine additional evidence to confirm secure deletion of sensitive data. Such evidence may include (but is not necessarily limited to) memory and storage dumps from development systems, evidence from memory traces from emulated systems, or evidence from physical extraction of data performed on-site by the software vendor.*	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that sensitive data stored in persistent data stores is rendered irretrievable upon secure deletion.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
3.5 Transient sensitive data is securely deleted from temporary storage facilities automatically by the software once the purpose for which it is retained is satisfied.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
3.5.a The assessor shall examine evidence to identify the methods implemented to render transient sensitive data irretrievable and to confirm that sensitive data is unrecoverable after the process is complete. ***Note:*** *This includes data which may be stored only temporarily in program memory / variables during operation of the software.*	**R1** Identify the evidence obtained that details the methods implemented to render sensitive data stored in transient data stores irretrievable upon secure deletion.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
3.5.b The assessor shall examine evidence and test the software to identify any platform or implementation level issues that complicate the erasure of such transient sensitive data, such as abstraction layers between the code and the hardware execution environment, and to confirm that methods have been implemented to minimize the risk posed by these complications.	**R1** Indicate whether known platform or implementation-level issues were discovered that complicate the secure deletion of sensitive data from transient data stores.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe the methods implemented to mitigate the risks associated with such complications.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
3.5.c The assessor shall test the software to identify any sensitive data residue in the execution environment and to confirm that the methods implemented are implemented correctly and enforced for all transient sensitive data. This analysis should accommodate for the data structures and methods used to store the sensitive data (for example, by examining file systems at the allocation level and translating data formats to identify sensitive data elements) and cover all non-transient sensitive data types.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that sensitive data retained in transient data stores is rendered irretrievable upon secure deletion.	
Note: *Where forensic testing of some or all aspects of the platform is not possible, the assessor should examine additional evidence to confirm secure deletion of sensitive data. Such evidence may include (but is not necessarily limited to) memory and storage dumps from development systems, evidence from memory traces from emulated systems, or evidence from physical extraction of data performed on-site by the software vendor.*	**R2** Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
3.6 The software does not disclose sensitive data through unintended channels.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
3.6.a The assessor shall examine evidence to confirm the software vendor has performed a thorough analysis to account for all sensitive data disclosure attack vectors including, but not limited to: • Error messages, error logs, or memory dumps. • Execution environments that may be vulnerable to remote side-channel attacks to expose sensitive data, such as attacks that exploit cache timing or branch prediction within the platform processor. • Automatic storage or exposure of sensitive data by the underlying execution environment, such as through swap-files, system error logging, keyboard spelling, and auto-correct features. • Sensors or services provided by the execution environment that may be used to extract or leak sensitive data, such as through use of an accelerometer to capture input of a passphrase to be used as a seed for a cryptographic key, or through capture of sensitive data through use of cameras or near-field communication (NFC) interfaces.	**R1** Identify the evidence obtained that details the software vendor's sensitive data disclosure attack vector analysis.			
	R2 Describe what the assessor observed in the evidence obtained that confirms the software vendor's analysis accounts for the attack vectors described in this test requirement.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
	R4 Identify the date when the software vendor's analysis was last performed or updated.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
3.6.b The assessor shall examine evidence, including the results of the analysis described in Test Requirement 3.6.a, and test the software to confirm that methods are implemented to protect against unintended disclosure of sensitive data. Such methods may include usage of cryptography to protect the data, or the use of blinding or masking of cryptographic operations (where supported by the execution environment).	**R1** Identify the evidence obtained that details the sensitive data stored, processed, or transmitted by the software that requires confidentiality protection.	
	R2 Describe the methods implemented to protect this data from unauthorized disclosure through the vectors identified in Test Requirement 3.6.a.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
3.6.c Where protection methods require user input or interaction, the assessor shall examine evidence to confirm that guidance on the proper configuration and use of such methods is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software requires or otherwise enables users to configure any of the protection methods identified in Test Requirement 3.6.b.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to configure these protection methods.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
3.6.d The assessor shall test the software to identify any sensitive data residue in the execution environment, and to confirm that protection methods are implemented correctly and the software does not expose or otherwise reveal sensitive data to unauthorized users.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that the protection methods identified in Test Requirement 3.6.b are implemented correctly and that sensitive data is not disclosed to unauthorized users.	
	R2 Identify the evidence obtained that confirms that the protection methods identified in Test Requirement 3.6.b are implemented correctly, and that the software does not leak or otherwise disclose sensitive data to unauthorized users or individuals.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 4: Critical Asset Protection Critical assets are protected from attack scenarios.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
4.1 Attack scenarios applicable to the software are identified. ***Note**: This control objective is an extension of Control Objective 10.1. Validation of both control objectives should be performed at the same time.*		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
4.1.a The assessor shall examine evidence to confirm that the software vendor has identified and documented relevant attack scenarios for the software.	**R1** Identify the evidence obtained that details the software vendor's analysis of potential threats and attack scenarios applicable to the assessed software.			
	R2 Identify the date when the software vendor's threat analysis was last performed or updated.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
4.1.b The assessor shall examine evidence to determine whether any specific industry-standard methods or guidelines were used to identify relevant attack scenarios. Where such industry standards are not used, the assessor shall confirm that the methodology used provides equivalent coverage for the attack scenarios applicable to the software under evaluation.	**R1** Identify the evidence obtained that details the software vendor's threat-modeling methodology.			
	R2 Indicate whether the software vendor's threat-modeling methodology is based on industry-standard methods or guidelines.	☐ Yes ☐ No		
	R3 If R2 is "Yes," then identify the industry-standard methods or guidelines used.			
	R4 If R2 is "No," then describe what the assessor observed in the evidence obtained that confirms the software vendor's methodology provides equivalent coverage to industry-standard methods.			
	R5 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
4.1.c The assessor shall examine evidence to confirm the following: • A formal owner of the software is assigned. This may be a role for a specific individual or a specific name, but evidence must clearly show an individual who is accountable for the security of the software. • A methodology is defined for measuring the likelihood and impact for any exploit of the system. • Generic threat methods and types that may be applicable to the software are documented. • All critical assets managed, and all sensitive resources used by the system are documented. • All entry and egress points for sensitive data, as well as the authentication and trust model applied to each of these entry/egress points, are documented. • All data flows, network segments, and authentication/privilege boundaries are documented. • All static IPs, domains, URLs, or ports required by the software for operation are documented. • Considerations for cryptography elements like cipher modes, and protecting against relevant attacks such as timing attacks, padded oracles, brute force, "rainbow table" attacks, and dictionary attacks against the input domain are documented.	**R1** Identify the individual assigned formal responsibility for the security of the assessed software.	
	R2 Identify the evidence obtained that details the software vendor's methodology for measuring the probability and impact of potential exploits.	
	R3 Describe what the assessor observed in the evidence obtained in Test Requirement 4.1.a that confirms the software vendor's threat analysis covers all software data flows, covers all data entry and egress points, and locations where sensitive data crosses trust boundaries.	
	R4 Describe what the assessor observed in the evidence obtained in Test Requirement 4.1.a that confirms the software vendor's threat analysis covers all software components, network segments, IPs, domains, URLs, and ports.	
	R5 Describe what the assessor observed in the evidence obtained in Test Requirement 4.1.a that confirms the software vendor's threat analysis covers all cryptographic implementations, including all algorithms and cipher modes used.	
	R6 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
4.1.c • Execution environment implementation specifics or assumptions, such as network configurations and operating system security configurations, are documented. • Considerations for the software execution environment, the size of the install base, and the attack surfaces that must be mitigated are documented. Examples of such attack surfaces may include insecure user prompts or protocol stacks, or the storage of sensitive data post authorization or using insecure methods.				
4.2 Software security controls are implemented to mitigate software attacks.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
4.2.a The assessor shall examine evidence to confirm that one or more mitigation methods are defined for each of the threats identified in Test Requirement 4.1.a or that justification for the lack of mitigations is provided.	**R1** Identify the evidence obtained that details the methods implemented to mitigate each of the threats identified in Test Requirement 4.1.a.			
	R2 Identify the evidence obtained that details the software vendor's justification(s) for any threats identified in Test Requirement 4.1.a that were not mitigated.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
4.2.b Where any mitigations rely on settings within the software, the assessor shall test the software to confirm that such settings are applied by default upon installation, initialization, or first use of the software.	**R1** Indicate whether any of the mitigations identified in Test Requirement 4.2.a rely on settings within the software.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that all such settings are applied upon software installation, initialization, or first use.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
4.2.c Where user input or interaction can disable, remove, or bypass any such mitigations, the assessor shall examine evidence and test the software to confirm that such action requires authentication and authorization and that guidance on the risk of such actions is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether users can disable, remove, or bypass any of the settings identified in Test Requirement 4.2.b.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that changes to those settings requires user authentication and authorization.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
4.2.d When any mitigations rely on features of the execution environment, the assessor shall examine evidence to confirm that guidance is provided to stakeholders on how to enable such settings in accordance with Control Objective 12.1.	**R1** Indicate whether any of the mitigations identified in Test Requirement 4.2.a rely on features of the execution environment.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to enable and configure the software to securely use these features.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
4.2.e Where the execution environment provides APIs to query the status of mitigation controls, the assessor shall test the software to confirm that software checks for these mitigations are in place and active prior to being launched and periodically throughout execution.	**R1** Indicate whether the software relies on APIs provided by the execution environment to query the status of software security controls.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe each of the software test(s) performed, including the tool(s) or method(s) used and the scope of each test, to confirm that checks are implemented to ensure that these security controls are in place and active upon and throughout software execution.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 5: Authentication and Access Control The software implements robust authentication and access control methods to protect the confidentiality, integrity, and resiliency of critical assets.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
5.1 Access to critical assets is authenticated.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
5.1.a The assessor shall examine evidence to confirm that authentication requirements are defined (i.e., type and number of factors) for all roles based on critical asset classification, the type of access (e.g., local, non-console, remote) and level of privilege. ***Note**: The assessor should refer to evidence obtained in the testing of Control Objective 1.3 to determine the classifications for all critical assets.*	**R1** Identify the evidence obtained that details all authentication methods relied upon by the software.			
	R2 Describe the software vendor's methodology for defining authentication requirements and whether authentication methods differ based on the types of critical assets accessed and the access privileges required.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
5.1.b The assessor shall examine evidence and test the software to confirm that access to critical assets is authenticated and authentication mechanisms are implemented correctly.	**R1** Describe the assessment activities performed to confirm that access to all critical assets is authenticated, and that all authentication mechanisms are implemented correctly.			
	R2 Describe what the assessor observed in the evidence obtained that confirms that access to all critical assets is authenticated.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
5.1.c Where the software recommends, suggests, relies on, or otherwise supports the use of external mechanisms (such as third-party VPNs, remote desktop features, etc.) to provide secure non-console access to the system on which the software is executed or directly to the software itself, the assessor shall examine evidence to confirm that guidance on how to configure authentication mechanisms correctly is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software relies on or supports the use of external authentication mechanisms.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to configure the software to securely use such authentication mechanisms.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
5.1.d The assessor shall examine evidence to confirm that sensitive data associated with authentication credentials, including public keys, is identified as a critical asset.	**R1** Identify the evidence obtained that confirms that all data associated with authentication credentials, including public keys, is appropriately protected.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
5.2 Access to critical assets requires unique identification.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
5.2.a The assessor shall examine evidence and test the software to confirm that all implemented authentication methods require unique identification.	**R1** Describe the assessment activities performed and what the assessor observed in the evidence obtained that confirms that all authentication mechanisms relied upon by the software require unique user identification.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
5.2.b Where interfaces, such as APIs, allow for automated access to critical assets, the assessor shall examine evidence and test the software to confirm that unique identification of different programs or systems accessing the critical assets is required (for example, through use of multiple public keys) and that guidance on configuring a unique credential for each program or system is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software provides or otherwise facilitates automated API access to critical assets.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that confirms that unique identification is required for each different program and system accessing these APIs.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
5.2.c Where identification is supplied across a non-console interface, the assessor shall test the software to confirm that authentication credentials are protected from attacks that attempt to intercept them in transit.	**R1** Indicate whether any authentication credentials (user, API, etc.) are supplied across a non-console interface.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe the methods implemented within or by the software to protect these authentication credentials from attempts to intercept them in transit.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
5.2.d The assessor shall examine evidence to confirm that the guidance provided to stakeholders per Control Objective 12.1 specifically notes that identification and authentication parameters must not be shared between individuals, programs, or in any way that prevents the unique identification of each access to a critical asset.	**R1** Identify the evidence obtained that details the software vendor's guidance on the proper use and protection of user authentication credentials.	
	R2 Describe any other assessment activities performed and/or findings for this control objective.	

5.3 Authentication methods (including session credentials) are sufficiently strong and robust to protect authentication credentials from being forged, spoofed, leaked, guessed, or circumvented.	**In Place**	**Not in Place**	**N/A**
	☐	☐	☐

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
5.3.a Using information obtained in Test Requirement 4.1.a, the assessor shall examine evidence to confirm that authentication methods implemented by the software are evaluated to identify known vulnerabilities or attack methods involving the authentication method and how the implementation of these methods mitigates against such attacks. The assessor shall also confirm that the evidence examined demonstrates the implementation used in the software was considered. For example, a fingerprint may be uniquely identifiable to an individual, but the ability to spoof or otherwise bypass such technology can be highly dependent on the way the solution is implemented.	**R1** Identify the evidence obtained that demonstrates that all authentication methods implemented by the software are evaluated to determine whether they contain known vulnerabilities.	
	R2 Describe how the implementation of these authentication methods mitigates vulnerabilities common to those methods.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
5.3.b The assessor shall examine evidence to confirm that the implemented authentication methods are robust, and that the robustness of the authentication methods was evaluated using industry-accepted methods. ***Note:*** *The vendor assessment and robustness justification include consideration of the full path of the user credentials, from any input source (such as a Human Machine Interface or other program), through transition to the execution environment of the software (including any switched/network transmissions and traversal through the execution environment's software stack before being processed by the software itself).*	**R1** Identify the evidence obtained that details the software vendor's analysis of the implemented authentication methods and their ability to resist attacks common to such methods.	
	R2 Describe how the software vendor evaluates the robustness of each of the implemented authentication methods and how the software vendor determines whether the authentication credentials are sufficiently strong to resist attacks.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
5.3.c The assessor shall test the software to confirm that the authentication methods are implemented correctly and do not expose vulnerabilities.	**R1** Describe each of the software tests performed in support of this test requirement, including the tool(s) or method(s) used and the scope of each test, to confirm that all authentication methods implemented by the software are implemented correctly and do not contain or otherwise expose vulnerabilities.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
5.4 By default, all access to critical assets is restricted to only those accounts and services that require such access.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
5.4.a The assessor shall examine evidence to confirm that information is maintained that identifies and justifies the required access for all critical assets.	**R1** Identify the evidence obtained that details the access privileges granted to critical assets by default, and the software vendor's justification for granted such access.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
5.4.b The assessor shall examine evidence and test the software to identify the level of access that is provided to critical assets and to confirm that such access correlates with the evidence examined in Test Requirement 5.4.a. Testing to confirm access to critical assets is properly restricted should include attempts to access critical assets through user accounts, roles, or services which should not have the required privileges.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that the access privileges granted to critical assets by default aligns with the evidence obtained in Test Requirement 5.4.a.			
	R2 Describe what the assessor observed in the evidence obtained through software testing that confirms access to critical assets is appropriately restricted to only those user accounts, roles, and services that require such access.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 6: Sensitive Data Protection Sensitive data is protected at rest and in transit.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
6.1 Sensitive data is secured anywhere it is stored.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
6.1.a The assessor shall examine evidence to confirm that protection requirements for all sensitive data are defined, including requirements for rendering sensitive data with confidentiality considerations unreadable anywhere it is stored persistently.	**R1** Identify the evidence obtained that details the integrity and confidentiality protection requirements for all sensitive data identified in Test Requirement 1.1.a.			
	R2 Describe any other testing activities performed and/or findings for this test requirement.			
6.1.b The assessor shall examine evidence and test the software to confirm that security controls are implemented to protect sensitive data during storage and that they address all defined protection requirements and identified attack scenarios. ***Note:*** *The assessor should refer to evidence obtained in the testing of Control Objective 1.1 to determine all sensitive data retained by the software, and Control Objective 4.1 to identify all attack scenarios applicable to the software.*	**R1** Identify the evidence obtained that details the security controls implemented to protect sensitive data during storage.			
	R2 Describe what the assessor observed in the evidence obtained that confirms the implemented security controls address all the protection requirements identified in Test Requirement 6.1.a.			
	R3 Describe what the assessor observed in the evidence obtained that confirms the implemented security controls address all applicable threats and attack scenarios identified in Test Requirement 4.1.a.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
6.1.c Where cryptography is used for securing sensitive data, the assessor shall examine evidence and test the software to confirm that methods implementing cryptography for securing sensitive data comply with Control Objective 7.	**R1** Indicate whether the software relies on cryptography to protect stored sensitive.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the cryptographic algorithms and cipher modes used or relied upon by the software.	
	R3 Describe what the assessor observed in the evidence obtained that confirms that each of the cryptographic algorithms and cipher modes used or relied upon complies with all applicable requirements within Control Objective 7.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	
6.1.d Where index tokens are used for securing sensitive data, the assessor shall examine evidence and test the software to confirm that these are generated in a way that ensures there is no correlation between the value and the sensitive data that is being referenced (without access to the software to perform the correlation as part of a formally defined and assessed feature of that software, such as "de-tokenization").	**R1** Indicate whether index tokens are used or otherwise relied upon to protect stored sensitive data.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe how the index tokens are generated in a way that ensures there is no correlation between the token value and the sensitive data being referenced.	
	R3 Describe any other assessment activities performed and/or findings for this control objective.	
6.1.e Where protection methods rely on the security properties of the execution environment, the assessor shall examine evidence and test the software to confirm that these security properties are valid for all platforms where the software is intended to be deployed.	**R1** Indicate whether software protection methods rely on the security properties of the execution environment to protect stored sensitive data.	☐ Yes ☐ No
	R2 If R1 is "Yes,' then describe what the assessor observed in the evidence obtained that confirms the security properties are valid for all platforms where the software is intended to be deployed.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
6.1.f Where protection methods rely on the security properties of third-party software, the assessor shall examine evidence and test the software to confirm that there are no unmitigated vulnerabilities or issues with the software providing the security properties.	**R1** Indicate whether implemented software protection methods rely on the security properties of third-party software to protect stored sensitive data.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms there are no unmitigated vulnerabilities in the third-party software.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
6.2 Sensitive data is secured during transmission.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
6.2.a The assessor shall examine evidence to identify the locations within the software where sensitive data is transmitted outside of the physical execution environment and to confirm protection requirements for the transmission of all sensitive data are defined.	**R1** Identify the evidence obtained that details the locations within the software where sensitive data is transmitted outside of the physical execution environment.			
	R2 Identify the evidence obtained that details the protection requirements for sensitive data transmitted outside of the physical execution environment.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
6.2.b The assessor shall examine evidence and test the software to confirm that for each of the ingress and egress methods that allow for transmission of sensitive data outside of the physical execution environment, the data is encrypted with strong cryptography prior to transmission or is transmitted over an encrypted channel using strong cryptography.	**R1** Describe what the assessor observed in the evidence obtained that confirms that sensitive data transmitted outside of the execution environment is encrypted using strong cryptography.	
Note: *The assessor should refer to evidence obtained in the testing of Control Objective 1.1 to determine the sensitive data stored, processed, or transmitted by the software.*	**R2** Describe any other assessment activities performed and/or findings for this test requirement.	
6.2.c Where third-party or execution-environment features are relied upon for the security of the transmitted data, the assessor shall examine evidence to confirm that guidance on how to configure such features is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software relies on third-party software or features of the execution environment to protect sensitive data during transmission.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to configure the assessed software to use these features in a secure manner.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
6.2.d Where transport layer encryption is used to secure the transmission of sensitive data, the assessor shall examine evidence and test the software to confirm that all ingress and egress methods enforce a secure version of the protocol with end-point authentication prior to transmission.	**R1** Indicate whether transport layer encryption is relied upon to protect sensitive data during transmission.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that all applicable ingress and egress methods enforce a secure version of the protocol with end-point authentication prior to transmission.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
6.2.e Where the methods implemented for encrypting sensitive data allow for the use of different types of cryptography or different levels of security, the assessor shall examine evidence and test the software, including capturing software transmissions, to confirm the software enforces the use of strong cryptography at all times during transmission.	**R1** Indicate whether the encryption methods implemented to protect sensitive data during transmission allow for the use of different types of cryptography or cryptography with different effective key strengths.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the method(s) used or relied upon by the software to ensure that strong cryptography is always enforced where sensitive data is transmitted outside of the execution environment.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
6.3 Use of cryptography meets all applicable cryptography requirements within this standard.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
6.3.a Where cryptography is relied upon (in whole or in part) for the security of critical assets, the assessor shall examine evidence and test the software to confirm that the use of cryptography is compliant to Control Objective 7. ***Note:*** *The assessor should refer to Control Objective 7 to identify all requirements for appropriate and correct implementation of cryptography.*	**R1** Indicate whether the software relies on cryptography for the protection of sensitive data during storage, processing, or transmission.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that all cryptography relied upon for the protection of sensitive data during storage, processing, or transmission complies (or can be configured to comply) with all applicable sections of Control Objective 7.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
6.3.b Where cryptographic methods provided by third-party software or aspects of the execution environment or platform on which the application is run are relied upon for the protection of sensitive data, the assessor shall examine evidence and test the software to confirm that guidance on configuring these methods during the installation, initialization, or first use of the software is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software relies on any cryptographic methods provided by third-party software or the execution environment to protect sensitive data.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to configure the assessed software to use these methods in a secure manner.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
6.3.c Where asymmetric cryptography such as RSA or ECC is used for protecting the confidentiality of sensitive data, the assessor shall examine evidence and test the software to confirm that private keys are not used for providing confidentiality protection to the data.	**R1** Indicate whether the software relies on asymmetric cryptography to encrypt sensitive data during storage, transmission, or processing.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained through examination and testing that confirms private keys are not used to protect the confidentiality of sensitive data during storage, transmission, or processing.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 7: Use of Cryptography Cryptography is used appropriately and correctly.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
7.1 Industry-standard cryptographic algorithms and methods are used for securing critical assets. Industry- standard cryptographic algorithms and methods are those recognized by industry-accepted standards bodies such as NIST, ANSI, ISO, and EMVCo. Cryptographic algorithms and parameters that are known to be vulnerable are not used.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
7.1.a The assessor shall examine evidence to determine how cryptography is used for the protection of critical assets and to confirm that: • Industry-standard cryptographic algorithms and modes of operation are used. • The use of any other algorithms is in conjunction with industry-standard algorithms. • The implementation of non-standard algorithms does not reduce the equivalent cryptographic key strength provided by the industry-standard algorithms.	**R1** Identify the evidence obtained that details the cryptographic algorithms and cipher modes relied upon by the software for the protection of sensitive data.			
	R2 Indicate whether any of these algorithms or cipher modes are considered proprietary or are not generally recognized as industry-standard methods.	☐ Yes ☐ No		
	R3 If R2 is "Yes," then describe how the implementation of these cryptographic algorithms ensures an effective minimum key strength equivalent to industry-standard methods.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
7.1.b The assessor shall examine evidence, including the vendor threat information obtained in Test Requirement 4.1.a, and test the software to confirm that: • Only documented cryptographic algorithms and modes of operation are used in the software. • Protection methods are implemented to mitigate common attacks on cryptographic implementations (for example, the use of the software as a decryption oracle, brute-force or dictionary attacks against the input domain of the sensitive data, the re-use of security parameters such as IVs, or the re-encryption of multiple datasets using linearly applied key values, such as XOR'd key values in stream ciphers or one-time pads).	**R1** Identify the evidence obtained that confirms that only documented cryptographic algorithms and cipher modes are relied upon by the software for the protection of sensitive data.	
	R2 Identify the evidence obtained that confirms that protection methods are implemented to mitigate threats to the cryptographic algorithms and cipher modes relied upon for the protection of sensitive data.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
7.1.c Where cryptographic implementations require a unique value per encryption operation or session, the assessor shall examine evidence and test the software to confirm that the cryptographic implementations do not expose vulnerabilities. For example, this may include the use of a unique IV for a stream cipher mode of operation or a unique and random "k" value for a digital signature.	**R1** Indicate whether any of the cryptographic implementations relied upon for the protection of sensitive data require a unique value per encryption operation or session.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms these implementations do not expose or otherwise contain vulnerabilities.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
7.1.d Where padding is used prior to or during encryption, the assessor shall examine evidence and test the software to confirm that the encryption operation always incorporates an industry-accepted standard padding method.	**R1** Indicate whether the software relies upon padding methods prior to or during encryption operations involving sensitive data.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that only industry-standard padding methods are used.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
7.1.e Where hash functions are used to protect sensitive data, the assessor shall examine evidence and test the software to confirm that: • Only approved, collision-resistant hash algorithms and methods are used for this purpose, and • A salt value of appropriate strength that is generated using a secure random number generator is used to ensure the resultant hash has sufficient entropy. ***Note:*** *The assessor should refer to Control Objective 7.3 for more information on secure random number generators.*	**R1** Indicate whether the software relies upon hash functions for the protection of sensitive data.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that only industry-standard, collision-resistant hashing algorithms are used.	
	R3 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that only salt values of appropriate strengths that are generated using a secure random number generator are used.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
7.2 The software supports industry-standard key management processes and procedures. Industry-standard key management processes and procedures are those recognized by industry standards bodies, such as NIST, ANSI, and ISO.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
7.2.a The assessor shall examine evidence to confirm that information is maintained that describes the following for each key specified in the inventory: • Key label or name • Key location • Effective date • Expiration date • Key purpose/type • Key generation method/algorithm used • Key length	**R1** Identify the evidence obtained that details the characteristics of each cryptographic key relied upon by the software for the protection of sensitive data.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
7.2.b The assessor shall examine evidence and test the software to validate the evidence examined in Test Requirement 7.2.a and to confirm that: • All cryptographic keys that are used for providing security to critical assets (confidentiality, integrity, and authenticity) and other security services to the software have a unique purpose, and that no key is used for both encryption and authentication operations. • All keys have defined generation methods, and no secret or private cryptographic keys relied upon for security of critical assets are shared between software instances, except when a common secret or private key is used for securing the storage of other cryptographic keys that are generated during the installation, initialization, or first use of the software (for example, white-box cryptography). • All cryptographic keys have an equivalent bit strength of at least 128 bits in accordance with industry standards. • All keys have a defined cryptoperiod aligned with industry standards, and methods are implemented to retire and/or update each key at the end of the defined cryptoperiod.	**R1** Describe what the assessor observed in the evidence obtained that confirms that all cryptographic keys that provide security to critical assets or other security services to the software have a unique purpose.	
	R2 Describe what the assessor observed in the evidence obtained through examination and testing that confirms that all secret or private cryptographic keys that are relied upon for the security of critical assets are not shared between software instances.	
	R3 Describe what the assessor observed in the evidence obtained that confirms that all cryptographic keys have an equivalent bit strength of at least 128 bits, or in accordance with industry standards where legacy implementations provide for less than 128 bits.	
	R4 Describe what the assessor observed in the evidence obtained that confirms that all cryptographic keys have a defined cryptoperiod, and that methods are implemented to retire or replace the keys at the end of their cryptoperiod.	
	R5 Describe what the assessor observed in the evidence obtained that confirms that the integrity and confidentiality of all secret and private cryptographic keys are appropriately protected where stored.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
7.2.b • The integrity and confidentiality of all secret and private cryptographic keys managed by the software are protected when stored (for example, encrypted with a key-encrypting key that is at least as strong as the data-encrypting key and is stored separately from the data-encrypting key, or as at least two full-length key components or key shares, in accordance with an industry-accepted method). • All keys have a defined generation or injection process, and this process ensures sufficient entropy for the key. • All key-generation functions must implement one-way functions or other irreversible key-generation processes, and no reversible key calculation modes (such as key variants) are used to directly create new keys from an existing key.	**R6** Describe what the assessor observed in the evidence obtained that confirms that all keys have a defined generation or injection process, and that the process ensures sufficient entropy for the key.	
	R7 Describe what the assessor observed in the evidence obtained that confirms that all key-generation methods implement one-way functions or other irreversible key-generation processes, and that no reversible key calculation modes are used to create new keys from an existing key.	
	R8 Describe any other assessment activities performed and/or findings for this test requirement.	
7.2.c Where cryptography is used to protect a key, the assessor shall examine evidence and test the software to confirm that security is not provided to any key by a key of lesser strength (for example, by encrypting a 256-bit AES key with a 128-bit AES key).	**R1** Indicate whether the software relies on cryptography to protect other cryptographic keys during storage or transmission.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that all cryptographic keys used to protect other keys possess an equal or greater effective key strength as the key(s) they protect.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
7.2.d Where public keys are used by the system, the assessor shall examine evidence and test the software to confirm that the authenticity of all public keys is preserved.	**R1** Indicate whether the software relies on public keys for the protection of sensitive data.	☐ Yes ☐ No
	R2 If R1 is "Yes, then describe what the assessor observed in the evidence obtained that confirms that the authenticity of these public keys is preserved.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
7.2.e Where public or white-box keys are not unique per software instantiation the assessor shall examine evidence to confirm that methods and procedures to revoke and/or replace such keys (or key pairs) exist.	**R1** Indicate whether the software relies upon public or white-box keys that are not unique to each software instance.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that methods are implemented to enable all such keys to be revoked and/or replaced with a unique key per instance.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
7.2.f Where the software relies upon external files or other data elements for key material, such as for public TLS certificates, the assessor shall examine evidence to confirm that guidance on how to install such key material, including details noting any security requirements for such key material, is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software relies upon external files or other external sources for cryptographic key material.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to configure the software to use supported external sources in a secure manner.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
7.2.g Where public keys are manually loaded or used as root keys, the assessor shall examine evidence and test the software to confirm that the keys are installed and stored in a way that provides dual control (to a level that is feasible for the execution environment), preventing a single user from replacing a key to enable a man-in-the-middle attack or the allow for unauthorized decryption of stored data. Where complete dual control is not feasible (for example, due to a limitation of the execution environment), the assessor shall confirm that the methods implemented are appropriate to protect the public keys.	**R1** Indicate whether the software uses or relies upon public keys that are manually loaded or used as root keys.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms these keys are installed and stored in a manner that provides for dual control, or that protects the keys from unauthorized substitution or modification where dual control is infeasible.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
7.3 All random numbers used by the software are generated using only industry-standard random number generation (RNG) algorithms or libraries. Industry-standard RNG algorithms or libraries are those that meet industry standards for sufficient unpredictability (for example, *NIST Special Publication 800-22*).		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
7.3.a The assessor shall examine evidence and test the software to identify all random number generators used by the software and to confirm that all random number generation methods: • Use at least 128 bits of entropy prior to the output of any random numbers. • Ensure it is not possible for the system to provide or produce reduced entropy upon start-up or entry of other predictable states of the system.	**R1** Identify the evidence obtained that details all locations within the software where random numbers are required.			
	R2 Describe what the assessor observed in the evidence obtained that confirms that all random number generation methods implemented use at least 128 bits of entropy prior to the output of any random numbers from the random number generator.			
	R3 Describe what the assessor observed in the evidence obtained that confirms that sufficient entropy (at least 128 bits) is always provided or produced upon start-up or entry of other predictable states of the system.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
7.3.b Where third-party software, platforms, or libraries are used for all or part of the random number generation process, the assessor shall examine evidence (such as current publicly available literature) to confirm that the third-party software does not expose any vulnerabilities that may compromise its use for generating random values.	**R1** Indicate whether the software relies upon third-party software, platforms, or libraries for all or part of the random number generation process.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that the third-party software, platforms, or libraries do not contain or otherwise expose any known vulnerabilities that would compromise its ability to secure generate random numbers.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
7.3.c Where the software vendor relies on a previous assessment of the random number generator or source of initial entropy, the assessor shall examine evidence (such as the approval records of the previous assessment) to confirm that this scheme and specific approval include the correct areas of the software in the scope of its assessment, and that the vendor claims do not exceed the scope of the evaluation or approval of that software. For example, some cryptographic implementations approved under FIPS 140-2 or 140-3 require seeding from an external entropy source to correctly output random data.	**R1** Indicate whether the software relies upon any random number generators that have been previously assessed to ensure they comply with industry-accepted standards for random number generation.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that all areas within the assessed software where these random number generators are used are covered by the approvals, and do not exceed the scope of evaluation or approval of those random number generation functions.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
7.3.d Where the software vendor does not rely on a previous assessment of the random number generator or source of initial entropy, the assessor shall test the software to obtain 128MB of data output from each random number generator implemented in the system to confirm the lack of statistical correlation in the output. This data may be generated by the assessor directly, or supplied by the vendor, but the assessor must confirm that the generation method implemented ensures that the data is produced as it would be produced by the software during normal operation. ***Note:*** *The assessor can use the NIST Statistical Test Suite to identify statistical correlation in the random number generation implementation.*	**R1** Indicate whether the software relies upon any random number generators that have NOT been previously assessed to ensure they comply with industry-accepted standards for random number generation.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that there is a lack of statistical correlation in the output from these random number generators.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
7.4 Random values have entropy that meets the minimum effective strength requirements of the cryptographic primitives and keys that rely on them.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
7.4.a The assessor shall examine evidence and test the software to confirm that the methods used for the generation of all cryptographic keys and other material (such as IVs, "k" values for digital signatures, and so on) have entropy that meets the minimum effective strength requirements of the cryptographic primitives and keys.	**R1** Describe what the assessor observed in the evidence obtained that confirms that all methods used to generate cryptographic keys and other material have entropy that meets the minimum effective strength requirements of the cryptographic primitives and keys.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
7.4.b Where cryptographic keys are generated through processes which require direct user interaction, such as through the entry of a passphrase or the use of "random" user interaction with the software, the assessor shall examine evidence and test the software to confirm that these processes are implemented in such a way that they provide sufficient entropy. Specifically, the assessor shall confirm that: • Methods used for generating keys directly from a password/passphrase enforce an input domain that is able to provide sufficient entropy, such that the total possible inputs are at least equal to that of the equivalent bit strength of the key being generated (for example, a 32- hex-digit input field for an AES128 key). • Passphrases are passed through an industry-standard key-derivation function, such as PBKDF2 or bcrypt, which extends the work factor for any attempt to brute-force a passphrase value. The assessor shall confirm that a work factor of at least 10,000 is applied to any such implementation. • Guidance is provided to stakeholders in accordance with Control Objective 12.1 that includes instructions that any passphrase used must: – Be randomly generated itself using a valid and secure random process, and that an online random number generator must not be used for this purpose. – Not be implemented by a single person, such that one person has an advantage in recovering the clear key value, violating the requirements for split knowledge.	**R1** Indicate whether the software uses or relies upon cryptographic keys that are generated through a process that requires direct user interaction.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that the methods used for generating keys directly from user input enforce an input domain that can provide sufficient entropy.	
	R3 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that user input is passed through an industry-standard key-derivation function that extends the work factor for all brute force attempts a minimum of 10,000.	
	R4 Identify the evidence obtained that details the software vendor's guidance on generating keys this way in a secure manner.	
	R5 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 8: Activity Tracking All software activities involving critical assets are tracked.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
8.1 All access attempts and usage of critical assets are tracked and traceable to a unique user. ***Note**: This Secure Software Standard recognizes that some execution environments cannot support the detailed logging requirements in other PCI standards. Therefore, the term "activity tracking" is used here to differentiate the expectations of this standard with regards to logging from similar requirements in other PCI standards.*		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
8.1 The assessor shall examine evidence and test the software to confirm that all access attempts and usage of critical assets are tracked and traceable to a unique individual, system, or entity.	**R1** Identify the evidence obtained that details the mechanisms implemented to track all user interactions with the software involving critical assets.			
	R2 Describe the different types of user accounts supported by the software (e.g., individual-level, system-level, entity-level, etc.) and the types of software assets each type of account is generally able to access (e.g., internal functions, API endpoints, etc.).			
	R3 Describe how the software ensures all activity involving critical assets is traceable to a unique user.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
8.2 All activity is captured in sufficient and necessary detail to accurately describe the specific activities that were performed, who performed them, the time they were performed, and the critical assets that were affected.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
8.2.a The assessor shall examine evidence and test the software to confirm that the tracking method(s) implemented capture specific activity performed, including: • Enablement of any privileged modes of operation. • Disabling of encryption of sensitive data. • Decryption of sensitive data. • Exporting of sensitive data to other systems or processes. • Failed authentication attempts. • Disabling or deleting a security control or altering security functions.	**R1** Identify the evidence obtained that details the specific activities involving critical assets that are captured by activity tracking mechanisms and confirms that the activities specified in this test requirement are covered.			
	R2 Indicate whether there are any limitations that complicate the software's ability to capture the activities specified in this test requirement.	☐ Yes ☐ No		
	R3 If R2 is "Yes," then describe the technical constraints that complicate the software's ability to capture the activities specified in this test requirement.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			
8.2.b The assessor shall examine evidence and test the software to confirm that the tracking method(s) implemented provide the following: • A unique identification for the individual, system, or entity accessing or using critical assets. • A timestamp for each tracked event. • Details on what critical asset has been accessed.	**R1** Identify the evidence obtained that details the user and activity data captured by tracking mechanisms in relation to the activities specified in Test Requirement 8.2.a.			
	R2 Describe what the assessor observed in the evidence obtained that confirms that, at a minimum, the user and activity data specified in this test requirement are captured for each of the activities specified in Test Requirement 8.2.a.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
8.2.c The assessor shall test the software to confirm that confidential data is not directly recorded in the tracking data.	**R1** Describe how the assessor confirmed that clear-text confidential data (i.e., sensitive data with confidentiality protection requirements) is not directly recorded in the output from activity tracking mechanisms.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
8.3 The software supports secure retention of detailed activity records.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
8.3.a Where the activity records are managed by the software, including only temporarily before being passed to other systems, the assessor shall examine evidence and test the software to confirm that the protection methods are implemented to protect completeness, accuracy, and integrity of the activity records.	**R1** Indicate whether the software maintains its own activity tracking records (even if only temporarily).	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the methods implemented by the software to ensure the completeness, accuracy, and integrity of its activity tracking records.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
8.3.b Where the software utilizes external or third-party systems for the maintenance of tracking data, such as a log server, the assessor shall examine evidence to confirm that guidance on the correct and complete setup and/or integration of the software with the external or third-party system(s) is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software relies upon or supports the use of external and/or third-party activity tracking mechanisms.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to configure the software to use these activity tracking mechanisms in a secure manner.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
8.3.c The assessor shall test the software to confirm methods are implemented to secure the authenticity of the tracking data during transmission to the log storage system, and to confirm that this protection meets the requirements of this standard (for example, authenticity parameters must be applied using strong cryptography) and any account or authentication parameters used for access to an external logging system are protected.	**R1** Describe what the assessor observed in the evidence obtained that confirms that the integrity of activity tracking data and records is always maintained.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
8.4 The software handles failures in activity-tracking mechanisms such that the integrity of existing activity records is preserved.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
8.4.a The assessor shall examine evidence and test the software to confirm that the failure of the activity-tracking mechanism(s) does not violate the integrity of existing records by confirming that: • The software does not overwrite existing tracking data upon a restart of the software. Each new start shall only append to existing datasets or shall create a new tracking dataset. • Where unique dataset names are relied upon for maintaining integrity between execution instances, the implementation ensures that other software (including another instance of the same software) cannot overwrite or render invalid existing datasets.	**R1** Describe the protection methods implemented to ensure prevent existing activity tracking records and data from being overwritten or corrupted when activity tracking mechanisms fail.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
8.4.a: • The software applies, where possible, suitable file privileges to assist with maintaining the integrity of the tracking dataset (such as applying an append-only access control to a dataset once created). Where the software does not apply such controls, the assessor shall confirm reasonable justification exists describing why this is the case, why the behavior is sufficient, and what additional mitigations are applied to maintain the integrity of the tracking data.		
8.4.b The assessor shall examine evidence and test the software to confirm that the integrity of activity tracking records is maintained by: • Performing actions that should be tracked, force-closing and then restarting the software, and performing other tracked actions. • Performing actions that should be tracked, power-cycling the platform on which the software is executing, and then restarting the software and performing other tracked actions. • Locking access to the tracking dataset and confirming that the software handles the inability to access this dataset in a secure way, such as by creating a new dataset or preventing further use of the software. • Preventing the creation of new dataset entries by preventing further writing to the media on which the dataset is located (for example, by using media that has insufficient available space).	**R1** Describe each of the assessment activities performed, including the tool(s) or method(s) used and the scope of each test, to confirm that the integrity of activity tracking records is always maintained.	
	R2 Indicate whether any of the tests specified in this test requirement could not be performed.	☐ Yes ☐ No
	R3 If R2 is "Yes," then describe the constraints that exist that complicate the performance of these tests.	
	R4 If R2 is "Yes," then describe what the assessor observed in the evidence obtained that confirms such constraints do not affect the ability to maintain the integrity of activity tracking records and data.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
Where any of the tests above are not possible, the assessor shall interview personnel to confirm reasonable justification exists to describe why this is the case and shall confirm protections are in place to prevent such scenarios from affecting the integrity of the tracking records.	**R5** Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 9: Attack Detection Attacks are detected, and the impacts/effects of attacks are minimized.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
9.1 The software detects and alerts upon detection of anomalous behavior, such as changes in post-deployment configurations or obvious attack behavior.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
9.1.a The assessor shall examine evidence and test the software to confirm that methods are implemented to validate the integrity of software executables and any configuration options, files, and datasets that the software relies upon for operation such that unauthorized post-deployment changes are detected. Where the execution environment prevents this, the assessor shall examine evidence (including publicly available literature on the platform and associated technologies) to confirm that there are indeed no methods for validating authenticity, and that additional security controls are implemented to minimize the associated risk.	**R1** Describe the methods that are implemented or relied upon to validate the integrity of the software's execution and configuration files.			
	R2 Indicate whether there are any constraints that complicate the implementation of such methods.	☐ Yes ☐ No		
	R3 If R2 is "Yes," then describe the additional security controls that are implemented to mitigate the risk of not having these capabilities.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			
9.1.b The assessor shall examine evidence and test the software to confirm that integrity values used by the software and dataset(s) upon which it relies for secure operation are checked upon software execution, and at least every 36 hours thereafter (if the software continues execution during that time period).	**R1** Indicate whether the software relies on integrity values or datasets to ensure the integrity of software execution and configuration files.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the frequency with which the software checks these values.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
9.1.c Where cryptographic primitives are used by any anomaly-detection methods, the assessor shall examine evidence and test the software to confirm that the cryptographic primitives are protected.	**R1** Indicate whether the software relies on cryptographic primitives for anomaly-detection capabilities.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the methods implemented to protect cryptographic primitives.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
9.1.d Where stored values are used by any anomaly-detection methods, the assessor shall examine evidence and test the software to confirm that these values are considered sensitive data and are protected accordingly.	**R1** Indicate whether the software relies on stored values for anomaly-detection capabilities.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe the methods implemented to protect stored values from unauthorized modification or disclosure.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
9.1.e Where configuration or other dataset values can be modified by the software during execution, the assessor shall examine evidence and test the software to confirm that integrity protections are implemented to allow for this update while still ensuring dataset integrity can be validated after the update.	**R1** Indicate whether the software enables or otherwise supports the modification of integrity values or datasets used for anomaly detection during software execution.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe how the software enables these values and datasets to be updated without compromising the integrity of those values.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
9.1.f The assessor shall examine evidence and test the software to confirm that the software implements controls to prevent brute-force attacks on account, password, or cryptographic-key input fields (for example, input rate limiting).	**R1** Describe the methods implemented to mitigate brute-force attacks on authentication mechanisms and credentials, as well as cryptographic operations.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
9.1.g Where third-party tools or services are relied upon by the software to provide attack detection capabilities, the assessor shall examine evidence to confirm that guidance on how to configure such tools and services to support this control objective is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software relies on third-party tools or services to provide attack detection capabilities.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to configure the software to use the third-party tools or services in a manner that meets applicable security requirements within this standard.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 10: Threat and Vulnerability Management Payment software threats and vulnerabilities are identified, assessed, and managed appropriately.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
10.1 Software threats and vulnerabilities are identified, assessed, and addressed.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
10.1.a Using information obtained in Test Requirement 4.1.a, the assessor shall examine evidence to confirm that common attack methods against the software are identified. This may include platform-level, protocol-level, and/or language-level attacks.	**R1** Describe the methods used by the software vendor to identify and/or detect vulnerabilities in the software that could be exploited by an attacker.			
	R2 Identify the evidence obtained that details the software vendor's most recent analysis of potential vulnerabilities within the software.			
	R3 Describe any other assessment activities performed and/or findings from this test requirement.			
10.1.b The assessor shall examine evidence to confirm that the identified attacks are valid for the software and shall note where this does not include common attack methods detailed in industry-standard references such as OWASP and CWE lists.	**R1** Describe the methods used by the software vendor to confirm the presence of vulnerabilities in the assessed software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
10.1.c The assessor shall examine evidence to confirm that mitigations against each identified attack are implemented, and that the software release process includes ongoing validation of the existence of these mitigations.	**R1** Describe the software vendor's process for identifying, prioritizing, and implementing mitigations to address vulnerabilities in the assessed software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
10.2 Vulnerabilities in the software and third-party components are tested for and fixed prior to release.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
10.2.a The assessor shall examine evidence to confirm that robust testing processes are used throughout the software lifecycle to manage vulnerabilities in software and to verify that the mitigations used to secure the software against attacks remain in place and are effective.	**R1** Describe the methods used and the frequency with which testing is performed to ensure new and evolving vulnerabilities are detected and that the existing mitigations remain effective.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
10.2.b The assessor shall examine evidence including documented testing processes and output of several instances of the testing to confirm that the testing process: • Includes, at a minimum, the use of automated tools capable of detecting vulnerabilities both in software code and during software execution. • Includes the use of security testing tools that are suitable for the software architecture, development languages, and frameworks used in the development of the software. • Accounts for the entire code base and detects vulnerabilities in third-party, open-source, or shared components and libraries. • Accounts for common vulnerabilities and attack methods. • Demonstrates a history of finding software vulnerabilities and remediating them prior to software release.	**R1** Describe how the software vendor uses automated tools to detect vulnerabilities in both the software code and during software execution.			
	R2 Describe how the software vendor's vulnerability testing processes cover the entire code base, including any open-source or third-party code embedded in the assessed software.			
	R3 Describe what the assessor observed in the evidence obtained that demonstrates the software vendor's vulnerability testing process detects both existing, as well as new or evolving vulnerabilities throughout the software lifecycle.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
10.2.c Where evidence examined in Test Requirement 10.2.b shows the release of software with known vulnerabilities, the assessor shall examine further evidence to confirm that: • An industry-standard vulnerability-ranking system (such as CVSS) is used to classify/categorize vulnerabilities. • A remediation plan is maintained for all detected vulnerabilities that ensures vulnerabilities do not remain unmitigated for an indefinite period.	**R1** Describe the software vendor's methodology for classifying and/or categorizing software vulnerabilities.	
	R2 Describe how the software vendor ensures that known vulnerabilities do not remain unmitigated indefinitely.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 11: Secure Software Updates Software releases and updates to address vulnerabilities are provided in a secure and timely manner.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
11.1 Software updates to fix known vulnerabilities are made available to stakeholders in a timely manner.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
11.1.a The assessor shall examine evidence to confirm that: • Reasonable criteria are defined for releasing software updates to fix security vulnerabilities. • Security updates are made available to stakeholders in accordance with the defined criteria.	**R1** Describe the software vendor's process for determining when a software update is required to address security vulnerabilities, and how this relates to the software vendor's methodology for classifying and/or categorizing software vulnerabilities.			
	R2 Describe the methods used and the frequency (if applicable) with which the software vendor makes security updates available to stakeholders.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
11.1.b The assessor shall examine evidence, including update-specific security-testing results and details, to confirm that security updates are made available to stakeholders in accordance with the defined criteria. Where updates are not provided in accordance with the defined criteria, the assessor shall confirm that such instances are justified and reasonable.	**R1** Describe what the assessor observed in the evidence obtained that confirms that security updates are provided to stakeholders in a timely manner.			
	R2 Describe the software vendor's criteria and process for determining when to delay security updates to address known vulnerabilities.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
11.2 Software releases and updates are delivered in a secure manner that ensures the integrity of the software code.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
11.2.a The assessor shall examine evidence to confirm that the method(s) by which the vendor releases software updates maintain the integrity of the software code during transmission and installation.	**R1** Describe the methods used by the software vendor to ensure that the integrity of the software code is maintained throughout distribution and installation of software updates.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
11.2.b Where user input or interaction is required to validate the integrity of the software code, the assessor shall examine evidence to confirm that guidance on this process is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether the software requires user input or interaction to validate the integrity of software updates prior to implementation.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to validate the integrity of software updates.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
11.2.c Where the integrity method implemented is not cryptographically secure, the assessor shall examine evidence to confirm that the software distribution method provides a chain of trust, such as through use of a TLS connection that provides compliant cipher-suite implementations.	**R1** Indicate whether the methods used to validate the integrity of software updates are not cryptographically secure.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the methods used by the software or software vendor to ensure a chain-of-trust is maintained throughout the implementation of software updates.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
11.2.d The assessor shall examine vendor evidence to confirm that stakeholders are notified of software updates, and that guidance on how they may be obtained and installed is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Describe the methods used by the software vendor to notify stakeholders of the availability of software updates.	
	R2 Describe what the assessor observed in the evidence obtained that confirms guidance is provided to stakeholders on how to implement software updates.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
11.2.e The assessor shall examine evidence to confirm that stakeholders are notified when known vulnerabilities are detected in software that has not yet been updated with a fix. This includes vulnerabilities that may exist in third-party software and libraries used by the software. The assessor shall confirm that this process includes providing the stakeholders with suggested mitigations for any such vulnerabilities.	**R1** Describe the software's vendor criteria and process for notifying stakeholders of known vulnerabilities in the assessed software for which a fix is not yet available.	
	R2 Describe what the assessor observed in the evidence obtained that confirms the software vendor provides stakeholders with suggested mitigations to address known vulnerabilities in the software where security updates are not yet available.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
11.2.f The assessor shall examine evidence to confirm that the software update mechanisms cover all software, configuration files, and other metadata that may be used by the software for security purposes or which may in some way affect the security of the software.	**R1** Describe what the assessor observed in the evidence obtained that confirms that security updates are provided to address vulnerabilities throughout the entire code base, including vulnerabilities in configuration files and other metadata.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective 12: Software Vendor Implementation Guidance The software vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of the software.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
12.1 The software vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of its payment software.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
12.1.a The assessor shall examine evidence to confirm that the vendor creates and provides stakeholders, clear and sufficient guidance to allow for the secure installation, configuration, and use of the software.	**R1** Identify the evidence obtained that details the software vendor's guidance for stakeholders on how to install and/or configure the security features of the software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
12.1.b The assessor shall examine evidence to confirm that the guidance: • Includes details on how to securely and correctly install any third-party software that is required for the operation of the vendor software. • Provides instructions on the correct configuration of the platform(s) on which the software is to be executed, including setting security parameters and installation of any data elements (such as certificates). • Includes instructions for key management (for example, the use of keys and how they are distributed, loaded, removed, changed, and destroyed.) • Does not instruct the user to disable security settings or parameters within the installed environment, such as anti-malware software or firewall or other network-level protection systems.	**R1** Describe what the assessor observed in evidence obtained that confirms the software vendor provides guidance on how to securely configure the assessed software to use any required third-party software.			
	R2 Describe what the assessor observed in the evidence obtained that confirms the software vendor provides guidance on how to securely configure the assessed software for the platform(s) supported by the software.			
	R3 Describe what the assessor observed in the evidence obtained that confirms the software vendor provides guidance on how to install and maintain cryptographic keys managed by the software.			
	R4 Describe what the assessor observed in the evidence obtained that confirms the software vendor does require users to disable security services, settings, or parameters implemented in the software execution environment.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
12.1.b: • Does not instruct the user to execute the software in a privileged mode higher than what is required by the software. • Provides details on how to validate the version of the software and clearly indicates for which version(s) of the software the guidance is written. • Provides justification for any requirements in this standard that are to be assessed as not applicable. For each of these, the assessor shall confirm justification exists for why this is the case and shall confirm that it agrees with their understanding and the results of their software testing.	**R5** Describe what the assessor observed in the evidence obtained that confirms the software vendor does not instruct users to execute the software in higher privilege mode than required by the software.	
	R6 Describe what the assessor observed in the evidence obtained that confirms the guidance is written for specific version(s) of the software, and that the intended version(s) is clearly noted in the guidance.	
	R7 Describe any other assessment activities performed and/or findings for this test requirement.	

4.2 Account Data Protection Module

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective A.1: Sensitive Authentication Data Sensitive Authentication Data (SAD) is not retained after authorization.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
A.1.1 The software does not store sensitive authentication data after authorization (even if encrypted) unless the software is intended only for use by issuers or organizations that support issuing services.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
A.1.1 Using information obtained in Test Requirement 1.1.a in the Core Requirements section, the assessor shall examine evidence and test the software to identify all potential storage locations for Sensitive Authentication Data, and to confirm that the software does not store such data after transaction authorization is complete. This includes storage of SAD in temporary storage (such as volatile memory), semi-permanent storage (such as RAM disks), and non-volatile storage (such as magnetic and flash storage media). Where Sensitive Authentication Data is stored after authorization, the assessor shall examine evidence to confirm that the software is designed explicitly for issuing purposes or for use by issuers or organizations that support issuing services.	**R1** Indicate whether the software retains Sensitive Authentication Data (SAD) after transaction authorization is complete.	☐ Yes ☐ No		
	R2 If R1 is "No," then describe what the assessor observed that confirms SAD is not retained after transaction authorization.			
	R3 If R1 is "Yes," then describe the software vendor's justification for retaining SAD after authorization.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective A.2: Cardholder Data Protection Stored cardholder data is protected.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
A.2.1 The software vendor provides guidance to stakeholders regarding secure deletion of cardholder data after expiration of defined retention period(s).		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
A.2.1 The assessor shall examine evidence to confirm that guidance is provided to stakeholders in accordance with Control Objective 12.1 that details: • All locations where the software stores cardholder data. • How to securely delete cardholder data stored by the payment software, including cardholder data stored on underlying software or systems (such as in OS files or in databases). • How to configure the underlying software or systems to prevent the inadvertent capture or retention of cardholder data (for example, by system backup or restore points).	**R1** Identify the evidence obtained that details the software vendor's guidance on handling cardholder data.			
	R2 Describe what the assessor observed in the evidence obtained that confirms all locations where sensitive data is stored in the assessed software is identified in the vendor guidance.			
	R3 Describe what the assessor observed in the evidence obtained that confirms that the software vendor provides guidance on how to securely delete sensitive data from storage locations.			
	R4 Describe what the assessor observed in the evidence that confirms the software vendor provides guidance on how to configure the underlying platform to prevent the inadvertent capture or retention of cardholder data.			
	R5 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
A.2.2 The software provides features to restrict or otherwise mask all displays of PAN to the minimum number of digits required.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
A.2.2.a The assessor shall examine evidence to confirm that the software provides features that enable responsible parties to restrict or otherwise mask the display of PAN to the minimum number of digits required to meet a defined business need.	**R1** Describe the options available within the software to restrict the display of PAN.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
A.2.2.b The assessor shall examine evidence to confirm that all displays of PAN are completely masked by default, and that explicit authorization is required to display any digits of the PAN.	**R1** Describe the default masking settings for all PAN displays within the software.			
	R2 Describe the process to enable and authorize the display of PAN for users.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
A.2.2.c Where user input or interaction is required to configure PAN masking features and options, the assessor shall examine evidence to confirm that guidance on how to configure these features/options is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Describe what the assessor observed in the evidence obtained that confirms stakeholders are provided guidance on how to configure available PAN-masking features and options.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
A.2.2.d The assessor shall test the software to confirm that all displays of PAN are completely masked by default, and that explicit authorization is required to display any element of the PAN.	**R1** Describe each of the tests performed, including the tool(s) and/or method(s) used and the scope of each test, to confirm that all displays of PAN are completely masked by default, and that explicit authorization is required to display any element of the PAN.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
A.2.3 PAN is rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs) by using any of the following approaches: • Truncation (hashing cannot be used to replace the truncated segment of PAN). • Index tokens and pads (pads must be securely stored). • Strong cryptography with associated key-management processes and procedures.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
A.2.3.a The assessor shall examine evidence and test the software to confirm that methods are implemented to render PAN unreadable anywhere it is stored using the following methods: • Truncation. • Index tokens and pads, with the pads being securely stored. • Strong cryptography, with associated key-management processes and procedures. ***Note**: The assessor should examine several tables, files, log files, and any other resources created or generated by the software to verify the PAN is rendered unreadable.*	**R1** Describe the methods relied upon by the software to render PAN unreadable anywhere it is stored.			
	R2 Describe what the assessor observed in the evidence obtained that confirms hashing is not used to render PAN unreadable.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
A.2.3.b Where user input or interaction is required to configure methods to render PAN unreadable when stored, the assessor shall examine evidence to confirm that guidance on configuring these options is provided to stakeholders in accordance with Control Objective 12.1 and that the guidance includes the following: • Details of any configurable options for each method used to render cardholder data unreadable, and instructions on how to configure each method for all locations where cardholder data is stored. • A list of all instances where cardholder data may be output for storage outside of the payment application, and instructions that the implementing entity is responsible for rendering the PAN unreadable in all such instances. • Instruction that if debugging logs are ever enabled (for troubleshooting purposes) and they contain PAN, they must be protected, that debugging must be disabled as soon as troubleshooting is complete, and that debugging logs must be securely deleted when no longer needed.	**R1** Indicate whether user input or interaction is required to configure methods to render PAN unreadable where stored.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on rendering PAN unreadable where stored.	
	R3 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms the guidance identifies all configurable options available to render PAN unreadable where stored and provides instructions on how to configure each available option.	
	R4 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms the guidance identifies all locations where cardholder data may be output by the software and provides instructions on how to render PAN in these locations unreadable.	
	R5 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms instructions on how to render PAN unreadable where it is stored for troubleshooting purposes.	
	R6 Describe any other assessment activities performed and/or findings for this test requirement.	
A.2.3.c Where software creates both tokenized and truncated versions of the same PAN, the assessor shall examine evidence and test the software to confirm that the tokenized and truncated versions cannot be correlated to reconstruct the original PAN.	**R1** Indicate whether the software maintains both truncated and truncated versions of the same PAN.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe the methods implemented to ensure the tokenized and truncated versions of the same PAN cannot be correlated to reconstruct the original PAN.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
A.2.3.d Where software creates or generates files for use outside the software (for example, files generated for export or backup), including for storage on removable media, the assessor shall examine evidence and test the software to confirm that PAN is rendered unreadable.	**R1** Indicate whether the software (or the underlying platform) allows for PAN to be output to external files or media.	☐ Yes ☐ No
	R2 If R1 is "No," then describe what the assessor observed (or how the assessor determined) that PAN is not output to external files or media.	
	R3 If R1 is "Yes," then describe the methods implemented to ensure PAN is rendered unreadable in the external files or media.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	
A.2.3.e If the software vendor stores PAN for any reason (for example, because log files, debugging files, and other data sources are received from customers for debugging or troubleshooting purposes), the assessor shall examine evidence and test the software to confirm that PAN is rendered unreadable in accordance with this control objective.	**R1** Indicate whether the software vendor enables the output of PAN to vendor systems.	☐ Yes ☐ No
	R2 If R1 is "No," then describe what the assessor observed (or how the assessor determined) that the software vendor does not output PAN to vendor systems.	
	R3 If R1 is "Yes," then describe the methods implemented to render PAN unreadable before outputting it to vendor systems.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

4.3 Terminal Software Module

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective B.1: Terminal Software Documentation The software architecture is documented and includes diagrams that describe all software components and services in use and how they interact.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.1.1 The software vendor maintains documentation that describes all software components, interfaces, and services provided or used by the software.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.1.1 The assessor shall examine evidence to confirm that documentation is maintained that describes the software's overall design and function including, but not limited to, the following: • All third-party and open-source components, external services, and Application Programming Interfaces (APIs) used by the software. • All User Interfaces (UI) and APIs provided or made accessible by the software.	**R1** Identify the evidence obtained that details the software's overall design and function.			
	R2 Describe what the assessor observed that confirms the software design documentation covers all third-party and open-source components, external services, and APIs used by the software.			
	R3 Describe what the assessor observed that confirms the software design documentation covers all interfaces and APIs provided or made accessible by the software.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.1.2 The software vendor maintains documentation that describes all data flows and functions that involve sensitive data. ***Note**: This control objective is an extension of Control Objectives 1.1 and 1.2. Validation of these control objectives should be performed at the same time.*		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.1.2.a The assessor shall examine evidence to confirm that documentation is maintained that describes all sensitive data flows including, but not limited to, the following: • All sensitive data stored, processed, or transmitted by the software. • All locations where sensitive data is stored, including both temporary and persistent storage locations. • How sensitive data is securely deleted from storage (both temporary and persistent) when no longer needed.	**R1** Identify the evidence obtained that details all data flows involving sensitive data.			
	R2 Describe what the assessor observed in the evidence obtained that confirms it details all sensitive data stored, process, and transmitted by the software.			
	R3 Describe what the assessor observed in the evidence obtained that confirms it details all locations where sensitive data is stored, including in both transient and persistent data stores.			
	R4 Describe what the assessor observed in the evidence obtained that confirms it details the mechanisms used to render sensitive data irretrievable upon execution of secure deletion methods.			
	R5 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
B.1.2.b The assessor shall examine evidence to confirm that documentation is maintained that describes all functions that handle sensitive data including, but not limited to, the following: • All inputs, outputs, and possible error conditions for each function that handles sensitive data. • All cryptographic algorithms, modes of operation, and associated key management practices for all functions that employ cryptography for the protection of sensitive data.	**R1** Identify the evidence obtained that details all software functions that handle sensitive data.	
	R2 Describe what the assessor observed in the evidence obtained that confirms it details all inputs, outputs, and possible error conditions for each function that handles sensitive data.	
	R3 Describe what the assessor observed in the evidence obtained that confirms it details all cryptographic algorithms, modes of operation, and associated key management practices for all functions that employ cryptography for the protection of sensitive data.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.1.3 The software vendor maintains documentation that describes all configurable options that can affect the security of sensitive data.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.1.3 The assessor shall examine evidence to confirm that documentation is maintained that describes all configurable options provided or made available by the software that can impact the security of sensitive data including, but not limited to, the following: • All configurable options that could allow access to sensitive data. • All configurable options that could enable modification of any mechanisms used to protect sensitive data. • All remote access features, functions, and parameters provided or made available by the software. • All remote update features, functions, and parameters provided or made available by the software. • The default settings for each configurable option.	**R1** Identify the evidence obtained that details all configurable options available that can impact the security of sensitive data.			
	R2 Describe what the assessor observed in the evidence obtained that confirms it details all configurable options that facilitate access to sensitive data.			
	R3 Describe what the assessor observed in the evidence obtained that confirms it details all configurable options that facilitate modification of mechanisms used to protect sensitive data.			
	R4 Describe what the assessor observed in the evidence obtained that confirms it details all remote access features, functions, and parameters provided or made available by the software.			
	R5 Describe what the assessor observed in the evidence obtained that confirms it details all remote update features, functions, and parameters provided or made available by the software.			
	R6 Describe what the assessor observed in the evidence obtained that confirms it details the default settings for each configurable option.			
	R7 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective B.2: Terminal Software Design The software does not implement any feature that enables the security features, functions, and characteristics of the payment terminal to be circumvented or rendered ineffective.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.1 The software is intended for deployment and operation on payment terminals (PCI-approved POI devices).		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.1 The assessor shall examine evidence to determine the payment terminals upon which the software is to be deployed. For each of the payment terminals identified and included in the software assessment, the assessor shall examine the payment terminal's device characteristics and compare them with the following characteristics specified in the *PCI SSC's List of Approved PTS Devices* to confirm they match: • Model name/number • PTS approval number • Hardware version number • Firmware version number(s)	**R1** Identify the evidence obtained that details the PCI PTS POI devices supported by the software.			
	R2 Describe what the assessor observed in the evidence obtained that confirms the devices included in the software assessment match the characteristics of those same devices on the *PCI SSC's List of Approved PTS Devices*.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.2 The software uses only the external communication methods included in the payment terminal's PTS device evaluation. ***Note**: The payment terminal may provide an IP stack approved per the PTS Open Protocols module, or the device may provide serial ports or modems approved by the PTS evaluation to communicate transaction data encrypted by its PCI PTS SRED functions. Using any external communication methods not included in the PCI-approved POI device evaluation invalidates the PTS approval, and such use is prohibited for terminal software.*		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.2.a The assessor shall examine evidence (including source code) to determine whether the software supports external communications.	**R1** Indicate whether the software supports the use of external communication methods.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the communication methods included in the software assessment.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.2.b Where the software supports external communications, the assessor shall examine all relevant payment terminal documentation (including the payment terminal vendor's security guidance/policy) to determine which external communication methods were included in the payment terminal's PTS device evaluation.	**R1** Identify the evidence obtained that details the terminal vendor's security guidance or policy for the PCI PTS POI devices included in the software assessment.			
	R2 Identify the communication methods included in the PTS device evaluation for each of the PCI PTS POI devices included in the software assessment.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.2.c The assessor shall examine evidence (including source code) to confirm that the software uses only the external communication methods included in the payment terminal's PTS device evaluation and does not implement its own external communication methods or IP stack.	**R1** Describe what the assessor observed in the evidence obtained that confirms the software uses only the external communication methods included in the PTS device evaluations for those PCI PTS POI devices included in the software assessment and does not implement its own external communication methods or IP stack.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.2.1 Where the software relies on the Open Protocols feature of the payment terminal, the software is developed in accordance with the payment terminal vendor's security guidance/policy.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
B.2.2.1 The assessor shall examine all relevant payment terminal documentation (including the payment terminal vendor's security guidance/policy) and all relevant software vendor process documentation and software design documentation to confirm that the software is developed in accordance with the payment terminal vendor's security guidance/policy.	**R1** Indicate whether the software relies upon the Open Protocols features of the PCI PTS POI devices included in the software assessment.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms the software is developed in accordance with the payment terminal vendor's security guidance/policy for each of the PCI PTS POI devices included in the software assessment.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.2.2 The software does not circumvent, bypass, or add additional services or protocols to the Open Protocols of the payment terminal as approved and documented in the payment terminal vendor's security guidance/policy. This includes the use of: • Link Layer protocols • IP protocols • Security protocols • IP Services		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.2.2 The assessor shall examine evidence (including source code) to confirm that the software does not circumvent, bypass, or add additional services or protocols to the Open Protocols of the payment terminal as approved and documented in the payment terminal vendor's security guidance/policy. This includes the use of: • Link Layer protocols • IP protocols • Security protocols • IP Services	**R1** Describe what the assessor observed in the evidence obtained in Test Requirements B.2.2 through B.2.2.2 that confirms the software does not circumvent, bypass, or add any additional services or protocols to the Open Protocols features provided by the PCI PTS POI devices included in the software assessment.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.2.3 The software does not bypass or render ineffective any encryption methods or account data security methods implemented by the payment terminal in accordance with the payment terminal vendor's security guidance/policy.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.3.a The assessor shall examine evidence (including source code) to determine whether the software provides encryption of sensitive data. Where the software does provide such a function, the assessor shall confirm the software does not bypass or render ineffective any encryption methods or account data security methods implemented by the payment terminal as follows:	**R1** Indicate whether the software provides its own methods to facilitate the encryption of sensitive data.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the methods provided by the software to facilitate sensitive data encryption.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.3.b The assessor shall examine all relevant payment terminal documentation (including payment terminal vendor security guidance/policy) to determine which encryption methods are provided by the payment terminal.	**R1** Indicate whether the PCI PTS POI devices included in the software assessment provide methods to facilitate the encryption of sensitive data.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the encryption methods provided by the device(s).			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.3.c The assessor shall examine evidence (including source code) to confirm that the software does not bypass or render ineffective any encryption methods provided by the payment terminal in accordance with the payment terminal vendor's security guidance/policy.	**R1** Describe what the assessor observed in the evidence obtained that confirms the software does not bypass or render ineffective any encryption methods provided by the payment terminal.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.2.3.d Where the software provides encryption of sensitive data, but the payment terminal is not required to provide approved encryption methods (per the *PCI PTS POI Standard*), the assessor shall examine evidence (including source code) to confirm that the encryption methods used or implemented by the software for encrypting sensitive data provide "strong cryptography" and are implemented in accordance with Control Objectives 7.1 and 7.2.	**R1** Indicate whether the device approvals for the PCI PTS POI devices included in the software assessment require that their own encryption methods be used.	☐ Yes ☐ No		
	R2 If R1 is "No," then describe what the assessor observed in the evidence obtained that confirms the methods provided by the software to encrypt sensitive data provide for strong cryptography.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.4 The software uses only the random number generation function(s) included in the payment terminal's PTS device evaluation for all cryptographic operations involving sensitive data or sensitive functions where random values are required and does not implement its own random number generation function(s).		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
B.2.4.a The assessor shall examine evidence (including source code) to determine whether the software requires random values to be generated for any cryptographic operations involving sensitive data or sensitive functions.	**R1** Indicate whether the software relies on random values to be generated for cryptographic operations involving sensitive data or sensitive functions.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details all software requirements for random numbers and the methods used to generate them.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.4.b Where the software requires random values for cryptographic operations involving sensitive data or sensitive functions, the assessor shall examine all relevant payment terminal documentation (including payment terminal vendor security guidance/policy) to determine all of the random number generation functions included in the payment terminal's PTS device evaluation.	**R1** Identify the random number generation functions included in the device evaluations for each of the PCI PTS POI devices included in the software assessment.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.2.4.c The assessor shall examine evidence (including source code) to confirm that the software uses only the random number generation function(s) included in the payment terminal's PTS device evaluation for all cryptographic functions involving sensitive data or sensitive functions where random values are required and does not implement its own random number generation function(s).	**R1** Describe what the assessor observed in the evidence obtained that confirms the software uses only those random number generation functions included in the device approvals for the PCI PTS POI devices included in the software assessment.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.5 The software does not provide, through its own logical interface(s), the sharing of clear-text account data directly with other software. ***Note**: The software is allowed to share clear-text account data directly with the payment terminal's firmware.*		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.5.a The assessor shall examine evidence (including source code) to determine all logical interfaces of the software, including: • All logical interfaces and the purpose and function of each. • The logical interfaces intended for sharing clear-text account data, such as those used to pass clear-text account data back to the approved firmware of the payment terminal. • The logical interfaces not intended for sharing of clear-text account data, such as those for communication with other software.	**R1** Identify the evidence obtained that details all logical interfaces of the software and their intended purpose.			
	R2 Describe the logical interfaces intended for sharing clear-text account data.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.5.b The assessor shall examine evidence (including source code) to confirm that the software does not allow sharing of clear-text account data directly with other software through its own logical interfaces.	**R1** Describe the methods implemented to prevent or restrict the sharing of clear-text account data with other software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
B.2.5.c The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall test the software using all software functions that handle account data to confirm that the software does not allow the sharing of clear-text account data directly with other software through its own logical interfaces.	**R1** Describe each of the tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that the software does not allow the sharing of clear-text account data directly with other software through its own logical interfaces.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.2.6 The software uses and/or integrates all shared resources securely and in accordance with the payment terminal vendor's security guidance/policy.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.6.a The assessor shall examine evidence (including source code) to determine whether and how the software connects to and/or uses any shared resources provided by the payment terminal, and to confirm that: • The guidance required in Control Objectives 12.1 and B.5.1 includes detailed instructions for how to configure the software to ensure secure integration with shared resources. • The required guidance for secure integration with shared resources is in accordance with the payment terminal vendor's security guidance/policy.	**R1** Indicate whether the software relies on any shared resources provided by the PCI PTS POI devices that are included in the software evaluation.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance for how to configure the software to securely integrate with the shared resources.			
	R3 If R1 is "Yes," describe what the assessor observed in the evidence obtained that confirms the software integrates the shared resources securely in accordance with the applicable PCI PTS POI device guidance/policy.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.6.b The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall test the software using all software functions that use or integrate shared resources to confirm that any connections to or use of shared resources are handled securely.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the results of each test, to confirm that all software connections to and use of shared resources are handled securely.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.2.7 The software does not bypass or render ineffective any application segregation enforced by the payment terminal.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.7.a The assessor shall examine all relevant payment terminal documentation (including the payment terminal vendor's security guidance/policy) to determine whether and how application segregation is enforced by the payment terminal.	**R1** Identify the evidence obtained to support this test requirement.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.7.b The assessor shall examine evidence (including source code) to confirm that the software does not introduce any function(s) that would allow it to bypass or defeat any device- level application segregation controls.	**R1** Indicate whether any of the PCI PTS POI devices included in the software assessment provide for or enforce application segregation within the device.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms the software adheres to all application segregation provided or enforced by applicable PCI PTS POI devices.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.8 All software files are cryptographically signed to enable cryptographic authentication of the software files by the payment terminal firmware.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.2.8.a The assessor shall examine the guidance required in Control Objectives 12.1 and B.5.1 to confirm that it includes detailed instructions for how to cryptographically sign the software files in a manner that enables the cryptographic authentication of all such files by the payment terminal.	**R1** Identify the evidence obtained that details the software vendor's guidance on how to cryptographically sign software files in a manner that supports cryptographic authentication of the software by applicable PCI PTS POI devices.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
B.2.8.b The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall confirm that all software files are cryptographically signed in a manner that enables the cryptographic authentication of all software files.	**R1** Identify each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that all software files can be cryptographically signed in a manner that supports the cryptographic authentication of those files by the applicable PCI PTS POI devices.	
	R2 Identify the evidence obtained that confirms that all software files can be cryptographically signed in a manner that supports the cryptographic authentication of those files by the applicable PCI PTS POI devices.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
B.2.8.c Where the software supports the loading of files outside of the base software package(s), the assessor shall examine evidence and test the software to determine whether each of those files is cryptographically signed in a manner that enables the cryptographic authentication of those files by the payment terminal. For any files that cannot be cryptographically signed, the assessor shall justify why the inability to cryptographically sign such files does not adversely affect the security of the software or the underlying payment terminal.	**R1** Indicate whether the software supports the loading of files outside of the base software package.	☐ Yes ☐ No
	R2 If R1 is "No," then describe what the assessor observed that confirms the software does not support the loading of files outside of the base software package(s).	
	R3 If R1 is "Yes," then identify the evidence obtained that demonstrates that all such files can be cryptographically signed in a manner that supports the cryptographic authentication of those files by the applicable PCI PTS POI devices.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.2.8.d The assessor shall examine evidence (including source code) to determine whether and how the software supports EMV® payment transactions. Where EMV payment transactions are supported by the software, the assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall confirm that all EMV Certification Authority Public Keys are cryptographically signed in a manner that enables the cryptographic authentication of those files by the payment terminal.	**R1** Indicate whether the software supports EMV® payment transactions.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify evidence obtained that demonstrates that all EMV Certification Authority Public Keys can be cryptographically signed in a manner that enables the cryptographic authentication of those files by applicable PCI PTS POI devices.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.9 The integrity of software prompt files is protected in accordance with Control Objective B.2.8.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
B.2.9.a The assessor shall examine evidence (including source code) to determine whether the software supports the use of data entry prompts and/or prompt files. Where the software supports such features, the assessor shall confirm the software protects the integrity of those prompts as defined in Test Requirements B.2.9.b through B.2.9.c.	**R1** Indicate whether the software supports the use of data entry prompts or prompt files.	☐ Yes ☐ No		
	R2 Identify the evidence obtained to support these findings.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.2.9.b The assessor shall examine the guidance required in Control Objectives 12.1 and B.5.1 to confirm that it includes detailed instructions for stakeholders to cryptographically sign all prompt files in a manner that enables the cryptographic authentication of all such files in accordance with B.2.8.	**R1** If applicable, identify the evidence obtained that details the software vendor's guidance on how to cryptographically sign prompt files in a manner that supports cryptographic authentication of the software by applicable PCI PTS POI devices.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
B.2.9.c The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall confirm that all prompt files are cryptographically signed in a manner that enables the cryptographic authentication of those files by the payment terminal in accordance with B.2.8.	**R1** If applicable, describe each of the software tests performed, including the tool(s) and/or method(s) used and the scope of each test, to confirm that all prompt files are cryptographically signed in a manner that enables the cryptographic authentication of those files by the payment terminal in accordance with B.2.8.	
	R2 Identify the evidence obtained that confirms that all prompt files are cryptographically signed in a manner that enables the cryptographic authentication of those files by the payment terminal in accordance with B.2.8.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective B.3: Terminal Software Attack Mitigation Software security controls are implemented to mitigate software attacks.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
B.3.1 The software validates all user and other external inputs. ***Note**: Control Objectives B.3.1 through B.3.3 are extensions of Control Objective 4.2. Validation of these control objectives should be performed at the same time.*		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
B.3.1.a The assessor shall examine evidence (including source code) to identify all locations where the software accepts input data from untrusted sources. For each instance, the assessor shall confirm that input data is required to conform to a list of expected characteristics and that all input that does not conform to the list of expected characteristics is rejected by the software or otherwise handled securely.	**R1** Identify the evidence obtained that details all locations within the software where input data from external or untrusted sources is accepted.			
	R2 Describe the method(s) used or relied upon by the software to ensure that input data conforms to a set of expected characteristics.			
	R3 Describe how the software handles input data that does not conform to the expected characteristics.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			
B.3.1.b The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall test the software by attempting to supply each user or other external input with invalid or unexpected characteristics to confirm that the software validates all inputs and either rejects or securely handles all unexpected characteristics.	**R1** Identify each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm the findings in Test Requirement B.3.1.a.			
	R2 Identify the evidence obtained that demonstrates that the software validates all inputs and either rejects or securely handles all unexpected characteristics.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.3.1.1 All string values are validated by the software.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.3.1.1.a The assessor shall examine evidence (including source code) to identify all terminal software functions where string values are passed as inputs, and to confirm that all strings are checked for text or data that can be erroneously or maliciously interpreted as a command.	**R1** Identify the evidence obtained that details all locations within the software where string values from external or untrusted sources are accepted as inputs.			
	R2 Describe the method(s) used or relied upon by the software to prevent input data from external or untrusted sources from being interpreted as a command.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.3.1.1.b The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall test the software by attempting to supply each of the identified functions with data that includes commands to confirm that the software either rejects such inputs or otherwise handles such inputs securely.	**R1** Identify each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm the findings in Test Requirement B.3.1.1.a.			
	R2 Identify the evidence obtained that demonstrates that the software either rejects or securely handles input data that can be interpreted as a command.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.3.1.2 The software checks inputs and rejects or otherwise securely handles any inputs that violate buffer size or other memory allocation thresholds.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.3.1.2.a The assessor shall examine evidence (including source code) to identify all software functions that handle buffers and process data supplied from untrusted sources. For each of the noted functions, the assessor shall confirm that each of the identified functions: • Uses only unsigned variables to define buffer sizes. • Conducts checks to confirm that buffers are sized appropriately for the data they are intended to handle, including consideration for underflows and overflows. • Rejects or otherwise securely handles any inputs that violate buffer size or other memory allocation thresholds.	**R1** Identify the evidence obtained that details all the software functions that handle buffers and accept data from external or untrusted sources.			
	R2 Identify the evidence obtained that demonstrates that only unsigned variables are used to define buffer sizes.			
	R3 Describe how the software ensures that buffers are sized appropriately for the data they are intended to store.			
	R4 Describe how the software handles input data that violates buffer size or any other memory allocation thresholds.			
	R5 Describe any other assessment activities performed and/or findings for this test requirement.			
B.3.1.2.b The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall test the software by attempting to supply each noted function with inputs that violate buffer size thresholds to confirm that the software either rejects or securely handles all such attempts.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to validate the findings in Test Requirement B.3.1.2.a.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.3.2 Return values are checked, and error conditions are handled securely.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.3.2.a Using information obtained in Test Requirement 1.2.a, the assessor shall examine evidence (including source code) to identify all software functions that handle sensitive data. For each of the noted software functions, the assessor shall confirm that each function: • Checks return values for the presence of sensitive data. • Processes the return values in a way that does not inadvertently "leak" sensitive data.	**R1** Describe the methods used by the software to check return values for the presence of sensitive data.			
	R2 Describe the protection methods implemented to ensure return values are processed in a way that does not inadvertently "leak" sensitive data.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
B.3.2.b The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall test each software function that handles sensitive data by attempting to manipulate the software in a manner that generates an unhandled exception to confirm that error conditions do not expose sensitive data.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to validate the findings in Test Requirement B.3.2.a.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.3.3 Race conditions are avoided.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.3.3.a The assessor shall examine evidence (including source code) to identify all software functions that rely on synchronous processing. For each of the noted functions, the assessor shall confirm that protection mechanisms have been implemented in the software to mitigate race conditions.	**R1** Identify the evidence obtained that details the sensitive functions of the software that rely on synchronous processing of data.			
	R2 Describe the protection methods implemented to protect these functions from race conditions.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
B.3.3.b The assessor shall install and configure the software in accordance with the guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods, the assessor shall test each software function that relies on synchronous processing by attempting to generate a race condition (such as through specially crafted attacks intended to exploit the timing of synchronous events) to confirm that the software is resistant to such attacks.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to validate the findings in Test Requirement B.3.3.a.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective B.4: Terminal Software Security Testing The software is tested rigorously for vulnerabilities prior to each release.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.4.1 A documented process is maintained and followed for testing software for vulnerabilities prior to each update or release. ***Note**: This control objective is an extension of Control Objective 10.2. Validation of these control objectives should be performed at the same time.*		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.4.1.a The assessor shall examine evidence to confirm that the software vendor maintains a documented process in accordance with Control Objective 10.2 for testing the software for vulnerabilities prior to each update or release, and that the documented process includes detailed descriptions of how the vendor tests for the following: • The presence or use of any unnecessary ports and protocols. • The unintended storage, transmission, or output of any clear-text account data. • The presence of any default user accounts with default or static access credentials. • The presence of any hard-coded authentication credentials in code or in configuration files. • The presence of any test data or test accounts. • The presence of any faulty or ineffective software security controls.	**R1** Describe how the software is tested for the presence unnecessary ports and protocols and the frequency of this testing.			
	R2 Describe how the software is tested for the unintended storage, transmission, and output of clear-text account data and the frequency of this testing.			
	R3 Describe how the software is tested for the presence of built-in user accounts with default or static authentication credentials and the frequency of this testing.			
	R4 Describe how the software is tested for the presence of hard-coded authentication credentials and the frequency of this testing.			
	R5 Describe how the software is tested for the presence of test data or test accounts and the frequency of this testing.			
	R6 Describe how the software is tested for the presence of faulty or ineffective security features or functions and the frequency of this testing.			
	R7 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
B.4.1.b The assessor shall examine evidence to confirm that the software is tested for vulnerabilities prior to each release and that the testing covers the following: • The presence or use of any unnecessary ports and protocols. • The unintended storage, transmission, or output of any clear-text account data. • The presence of any default user accounts with static access credentials. • The presence of any hard-coded authentication credentials in code or in configuration files. • The presence of any test data or test accounts. • The presence of any faulty or ineffective software security controls.	**R1** Identify the evidence obtained that confirms the findings for this test requirement.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective B.5: Terminal Software Implementation Guidance The software vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of the software on applicable payment terminals.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.5.1 The software vendor provides implementation guidance on how to implement and operate the software securely for the payment terminals on which it is to be deployed. ***Note**: This control objective is an extension of Control Objective 12.1. Validation of these control objectives should be performed at the same time.*		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.5.1 The assessor shall examine evidence to confirm that guidance on how to securely implement and operate the software for all applicable payment terminals is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Identify the evidence obtained that details the software vendor's guidance on the implementation and operation of the software for applicable payment terminals.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.5.1.1 Implementation guidance includes detailed instructions for how to configure all available security options and parameters of the software.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.5.1.1 The assessor shall examine evidence to confirm that the required guidance includes detailed instructions on how to configure all available security options and parameters of the software in accordance with Control Objective B.1.3.	**R1** Describe what the assessor observed in the evidence obtained that confirms vendor guidance includes instructions on how to configure the security options and parameters of the software can be found.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.5.1.2 Implementation guidance includes detailed instructions for how to securely configure the software to use the security features and functions of the payment terminal where applicable.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.5.1.2 The assessor shall examine evidence to confirm that the required guidance includes detailed instructions on how to securely configure the software to use the security features and functions of the payment terminal where applicable.	**R1** Describe what the assessor observed in the evidence obtained that confirms vendor guidance includes instructions on configuring the software to use the security features and functions of applicable PCI PTS POI devices can be found.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.5.1.3 Implementation guidance includes detailed instructions for how to configure the software to securely integrate or use any shared resources provided by the payment terminal.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
B.5.1.3 The assessor shall examine evidence to confirm that the required guidance includes detailed instructions on how to configure the software to securely integrate or use any shared resources provided by the payment terminal in accordance with Control Objective B.2.6.	**R1** Describe what the assessor observed in the evidence obtained that confirms vendor guidance includes instructions on how to configure the software to use shared resources provided by applicable PCI PTS POI devices can be found.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.5.1.4 Implementation guidance includes detailed instructions on how to cryptographically sign the software files in a manner that enables the cryptographic authentication of all such files by the payment terminal.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
B.5.1.4 The assessor shall examine evidence to confirm that the required guidance includes detailed instructions on how to cryptographically sign the software files in a manner that enables the cryptographic authentication of all such files by the payment terminal in accordance with Control Objective B.2.8.	**R1** Describe what the assessor observed in the evidence obtained that confirms that vendor guidance includes instructions on how to cryptographically sign software files in a manner that enables cryptographic authentication of such files by applicable PCI PTS POI devices can be found.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
B.5.1.5 Implementation guidance includes instructions for stakeholders to cryptographically sign all prompt files.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.5.1.5 The assessor shall examine evidence to confirm that the required guidance includes detailed instructions for stakeholders to cryptographically sign all prompt files in accordance with Control Objective B.2.9.	**R1** Describe what the assessor observed in the evidence obtained that confirms that vendor guidance includes instructions on how to cryptographically sign prompt files.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
B.5.2 Implementation guidance adheres to payment terminal vendor guidance on the secure configuration of the payment terminal.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
B.5.2 The assessor shall examine evidence (including the payment terminal vendor's security guidance/policy and the guidance required in Control Objective B.5.1) to confirm that the guidance aligns with the payment terminal vendor's security guidance/policy.	**R1** Describe what the assessor observed in the evidence obtained that confirms the software vendor's guidance does not conflict with the payment terminal vendors' security guidance for the PCI PTS POI devices included in the software assessment.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

4.4 Web Software Module

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective C.1: Web Software Components & Services All components and services used by the software are identified and maintained in a manner that minimizes the exposure of vulnerabilities.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.1.1 All software components and services are documented or otherwise cataloged in a software bill of materials (SBOM).		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.1.1 The assessor shall examine evidence to confirm that information is maintained that describes all software components and services comprising the software solution, including: • All proprietary software libraries, packages, modules, and/or code packaged in a manner that enables them to be tracked as a freestanding unit of software. • All third-party and open-source frameworks, libraries, and code embedded in or used by the software during operation. • All third-party software dependencies, APIs, and services called by the software during operation.	**R1** Identify the evidence obtained that details the assessed software's bill of materials (SBOM).			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.1.2 The SBOM describes each of the primary components and services in use, as well as their secondary transitive component relationships and dependencies to the greatest extent feasible.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.1.2.a The assessor shall examine evidence to confirm that the SBOM describes all primary (top-level) components and services in use and all of their secondary transitive relationships and dependencies.	**R1** Describe how the SBOM differentiates between primary components and services and their secondary transitive dependencies.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.1.2.b The assessor shall test the software to confirm that the information provided in the SBOM accurately reflects the software components and services in use during software operation, including both primary components and services as well as their secondary transitive component relationships and dependencies. Where such dependencies and relationships are not identified and described in the SBOM, the assessor shall confirm that the absence of such information is justified and reasonable.	**R1** Identify each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to validate the evidence obtained in Test Requirement C.1.2.a.			
	R2 Indicate whether software testing identified any components or services used during software operation that were not reflected in the SBOM.	☐ Yes ☐ No		
	R3 If R2 is "Yes," then describe why the assessor considers it acceptable for these components or services to be excluded from the SBOM.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			
C.1.3 Where the software is provided "as a service," the SBOM includes information describing the software dependencies present in the production software execution environment to the greatest extent feasible.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.1.3.a The assessor shall examine evidence to confirm that the SBOM describes all dependencies present in the production software execution environment that the software relies upon for operation or to satisfy security requirements in this standard.	**R1** Indicate whether the software is provided "as-a-service".	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms that production software execution environment dependencies are noted in the SBOM.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
C.1.3.b The assessor shall examine evidence and test the software (to the extent possible) to confirm that the information provided in the SBOM accurately reflects the software dependencies present in the production software execution environment. Where such dependencies are not identified and described in the SBOM, the assessor shall confirm that the absence of such information is justified and reasonable.	**R1** Identify each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to validate the evidence obtained in Test Requirement C.1.3.a.	
	R2 Indicate whether software testing identified any components or services used during software operation that were not reflected in the SBOM.	☐ Yes ☐ No
	R3 If R2 is "Yes," then describe why the assessor considers it acceptable for these dependencies to be excluded from the SBOM.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.1.4 The SBOM includes sufficient information about each component or service to enable tracking each component or service across the software supply chain.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.1.4.a The assessor shall examine evidence to confirm that information is maintained in the SBOM that describes the following for each component and service in use, including secondary component relationships and dependencies: • The original source/supplier of the component or service. • The name of the component or service as defined by the original supplier. • A description of the relationship(s) between the component and service and other components/services embedded in or used by the software. • The version of the component or service as defined by the original supplier to differentiate it from previous or other versions. • The name of the author who designed/developed the component or service. • Any other identifiers provided by the original supplier to uniquely identify the component or service.	**R1** Describe the overall structure of the SBOM, the nomenclature and attributes used, and how the SBOM accounts for components and services.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.1.4.b The assessor shall examine evidence and test the software to confirm that the information provided in the SBOM is an accurate representation of the software components and services present in and/or in use by the software.	**R1** Describe what the assessor observed in the evidence obtained that confirms the SBOM is an accurate representation of the software components and services present in and/or in use by the software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.1.5 A new SBOM is created or generated each time the software is updated.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.1.5 The assessor shall examine evidence to confirm that a new SBOM is created or otherwise generated for each new release of the software.	**R1** Describe the software vendor's processes for generating SBOMs and how it ensures one is generated for each new software release.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.1.6 Vulnerabilities in third-party components and services are monitored and managed in accordance with Control Objective 10.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.1.6.a The assessor shall examine evidence to confirm that third-party components and services present in and/or in use by the software are regularly monitored for vulnerabilities in accordance with Control Objective 10.1.	**R1** Describe how the software vendor leverages the SBOM to monitor and manage vulnerabilities in third-party components and services.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.1.6.b The assessor shall examine evidence to confirm that vulnerabilities in third-party components and services are identified and are patched or otherwise mitigated in a timely manner in accordance with Control Objective 10.2.	**R1** Identify the evidence obtained that confirms that vulnerabilities in third-party components are patched or mitigated in a timely manner.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.1.7 Where software components and/or resources are hosted or maintained on third-party systems, such as content delivery networks (CDN), the authenticity of those components and resources is verified each time they are fetched.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.1.7.a Where software components and resources are fetched from external and/or third-party repositories, the assessor shall examine evidence to confirm that the authenticity of the software component is verified each time the component is fetched.	**R1** Indicate whether the software relies upon any software components or resources that are fetched from external or third-party repositories.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe how the software confirms the authenticity of the component or resource and the frequency of such checks.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
C.1.7.b The assessor shall test the software to confirm that the authenticity of all software components and resources fetched from third-party systems or repositories is verified each time they are fetched by the software.	**R1** If applicable, identify the software tests performed, including the tool(s) or method(s) used and the scope of each test, to validate the evidence obtained in Test Requirement C.1.7.a.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective C.2: Web Software Access Controls Software security controls are implemented to restrict access to Internet-accessible interfaces, functions, and resources to explicitly authorized users only.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.2.1 User access to sensitive functions and sensitive resources exposed through Internet-accessible interfaces is authenticated.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.2.1 Using information obtained in Test Requirements 1.2.a and 2.1.a in the Core Requirements, the assessor shall examine evidence to identify all sensitive functions and sensitive resources exposed through Internet-accessible interfaces.	**R1** Identify the evidence obtained that details all sensitive functions and sensitive resources that are exposed, or that may be exposed, through Internet-accessible interfaces.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.1.1 The methods implemented to authenticate user access to sensitive functions and sensitive resources use industry-standard mechanisms.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.2.1.1.a The assessor shall examine evidence to identify all methods implemented by the software to authenticate access to sensitive functions and sensitive resources.	**R1** Describe the method(s) relied upon by the software to authenticate access to the sensitive functions and sensitive resources identified in Test Requirement C.2.1.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.1.1.b The assessor shall examine evidence to confirm that the implemented methods use industry-standard mechanisms that are: • Provided by well-known and industry-accepted third-party suppliers; or • Designed and implemented in accordance with applicable industry standards or best practices.	**R1** Indicate whether any of the methods relied upon by the software to authenticate access to the sensitive functions and sensitive resources identified in Test Requirement C.2.1 are provided by third-party suppliers.	☐ Yes ☐ No		
	R2 If R1 is "Yes," describe what the assessor observed that confirms these methods are provided by well-known and industry-accepted third-party suppliers or is designed and implemented in accordance with industry standards and best practices.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
C.2.1.1.c Where sessions are used to authenticate user access to sensitive functions and sensitive resources, the assessor shall examine evidence to confirm that the sessions are handled in accordance with industry-recognized standards and best practices for secure session management.	**R1** Indicate whether the software relies on "sessions" to authenticate user access to the sensitive functions and sensitive resources identified in Test Requirement C.2.1.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms the use of "sessions" industry-recognized standards and best practices for secure session management.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
C.2.1.1.d Where tokens (for example, access tokens and refresh tokens) are used to authenticate user access to sensitive functions and sensitive resources, the assessor shall examine evidence to confirm that the tokens are handled in accordance with industry-recognized standards and best practices for secure token management.	**R1** Indicate whether the software relies on tokens to authenticate user access to the sensitive functions and sensitive resources identified in Test Requirement C.2.1.	☐ Yes ☐ No
	R2 If R1 is "Yes," then describe the types of tokens used to authenticate user access to the sensitive functions and sensitive resources identified in Test Requirement C.2.1.	
	R3 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms the use of tokens adheres industry-recognized standards and best practices for secure token management.	
	R4 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.2.1.2 The methods implemented to authenticate user access to sensitive functions and sensitive resources through Internet-accessible interfaces are sufficiently strong and robust to protect authentication credentials in accordance with Control Objective 5.3.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.2.1.2 Using information obtained in Test Requirement C.2.1.1.a, the assessor shall examine evidence to confirm that the authentication methods implemented are sufficiently strong and robust to protect authentication credentials in accordance with Control Objective 5.3 in the Core Requirements section.	**R1** Describe how the methods implemented to authenticate user access to the sensitive functions and sensitive resources identified in Test Requirement C.2.1 mitigate the likelihood of authentication credentials being forged, spoofed, guessed, or otherwise compromised by an unauthorized entity.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.1.3 Authentication decisions are enforced within a secure area of the software.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.2.1.3.a The assessor shall examine evidence to identify where within the software architecture authentication decisions are enforced.	**R1** Describe the locations within the software architecture where authentication decisions are enforced.			
	R2 Identify the evidence obtained that supports this finding.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.1.3.b The assessor shall examine evidence to confirm that all authentication decisions are enforced within a secure area of the software architecture.	**R1** Describe what the assessor observed in the evidence obtained that confirms that authentication decisions are enforced within a secure area of the software architecture.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.2.1.3.c The assessor shall examine evidence and test the software to confirm that client-side or browser-based functions, scripts, and data are never solely relied upon for authentication purposes.	**R1** Indicate whether client-side or browser-based functions, scripts, or data are used for authenticating access to software interfaces.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe how the software uses these functions, scripts, and data for authenticating access to software interfaces.			
	R3 Describe the methods implemented to protect these functions, scripts, and data from compromise or manipulation by an unauthorized entity.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.2 Access to all Internet-accessible interfaces is restricted to explicitly authorized users only.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.2.2.a Using information obtained in Test Requirement 2.1.a in the Core Requirements section, the assessor shall examine evidence to identify all software interfaces that are exposed to the Internet or that can be configured in a way that exposes them to the Internet.	**R1** Identify the evidence obtained that details the software interfaces that are exposed, or that could be configured in a way to expose them, to the Internet.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.2.b The assessor shall examine evidence to identify all methods used to authorize access to Internet-accessible interfaces.	**R1** Identify the methods used to restrict access to the software interfaces identified in Test Requirement C.2.2.a to only authorized users (for example, API keys, IP lists, attribute-based access control, etc.)			
	R2 Identify the evidence obtained that supports these findings.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
C.2.2.c The assessor shall examine evidence and test the software to confirm that each of these methods is: • implemented correctly; • appropriate for the types of users expected to use the interface; and • does not expose known vulnerabilities.	**R1** Describe what the assessor observed in the evidence obtained that confirms that the methods identified in Test Requirement C.2.2.b to restrict access to software interfaces are appropriate for the type(s) of interface provided and does not expose known vulnerabilities.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
C.2.2.d Where the methods used to authorize access to Internet-accessible interfaces is user configurable, or otherwise requires user input or interaction, the assessor shall examine evidence to confirm that appropriate guidance is made available to stakeholders in accordance with Control Objective 12.1 that describes the configurable options available and how to configure each method securely.	**R1** Indicate whether any of the methods identified in Test Requirement C.2.2.b requires or enables users to configure those methods.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the configurable options available and the software vendor's guidance on how to configure each method securely.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
C.2.2.e Where the methods used to authorize access to Internet-accessible interfaces are configured and controlled by the assessed entity, the assessor shall examine evidence to confirm that access to Internet-accessible interfaces is restricted to an appropriate set of explicitly authorized users (or entities).	**R1** Indicate whether any of the interfaces identified in Test Requirement C.2.2.a are managed by the assessed entity (for example, as-a-service).	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that demonstrates that access to the applicable interfaces is restricted to explicitly authorized users.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
C.2.2.f The assessor shall examine evidence and test the software to confirm that access to all Internet-accessible interfaces is restricted to explicitly authorized users only.	**R1** Identify the software tests performed, including the tool(s) or method(s) used and the scope of each test, to validate the findings in Test Requirements C.2.2.c and C.2.2.e.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
	R2 Describe what the assessor observed in the evidence obtained that confirms that access to the applicable interfaces is restricted to an appropriate set of explicitly authorized users.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.3 Access to all software functions and resources exposed through Internet-accessible interfaces is restricted to explicitly authorized users only.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.2.3 Using information obtained in Test Requirement C.2.2.a, the assessor shall examine evidence to identify all software functions and resources that are exposed, or that can be configured in a way that exposes them, through Internet-accessible interfaces.	**R1** Identify the evidence obtained that details all software functions or resources that are exposed, or that can be exposed, through APIs or other interfaces.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.3.1 The software ensures the enforcement of access control rules at both the function level and resource level with fine-grained access control capabilities.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.2.3.1.a Using information obtained in Test Requirement C.2.3, the assessor shall examine evidence to determine how the software controls access to individual functions and resources exposed (or potentially exposed) through Internet-accessible interfaces.	**R1** Describe the methods relied upon by the software to control access to sensitive functions and sensitive resources made accessible (or that can be configured to make them accessible) through APIs or other interfaces.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
C.2.3.1.b The assessor shall then examine evidence to identify the methods used to restrict access to the functions and resources exposed (or potentially exposed) through Internet-accessible interfaces and to confirm that each of these methods is: • implemented correctly; • appropriate for the type of function(s) and resource(s) provided; and • does not expose known vulnerabilities.	**R1** Describe what the assessor observed in the evidence obtained that confirms the methods described in Test Requirement C.2.3.1.a are implemented correctly and do not expose known vulnerabilities.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
C.2.3.1.c Where the methods used to authorize access to the functions and resources exposed (or potentially exposed) through Internet-accessible interfaces are user configurable or otherwise requires user input or interaction, the assessor shall examine evidence to confirm that guidance is made available to stakeholders in accordance with Control Objective 12.1 that describes the mechanisms and configurable options available to restrict access to the functions and resources exposed through these interfaces, and how to configure such mechanisms.	**R1** Indicate whether any of the methods described in Test Requirement C.2.3.1.a are user configurable.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on how to configure such methods securely.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
C.2.3.1.d Where the methods used to authorize access to the functions and resources exposed (or potentially exposed) through Internet-accessible interfaces is configured and controlled by the assessed entity, the assessor shall examine evidence to confirm that access to the functions and resources is restricted to an appropriate set of explicitly authorized users.	**R1** Indicate whether access to any of the functions and resources exposed, or potentially exposed, through exposed through APIs or other interfaces is controlled by the assessed software or software vendor.	☐ Yes ☐ No
	R2 If R1 is "Yes," then identify the evidence obtained that confirms access to all such functions and resources is restricted to any appropriate set of explicitly authorized users.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.2.3.1.e The assessor shall examine evidence and test the software to confirm that the methods used to restrict access to the functions and resources exposed (or potentially exposed) through Internet-accessible interfaces require users to be explicitly authorized prior to being granted such access.	**R1** Describe each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that access to functions and resources exposed through APIs or other interfaces requires users to be explicitly authorized before access is granted.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.3.2 Authorization rules are enforced upon each user request to access software functions and resources through Internet-accessible interfaces.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.2.3.2.a Using information obtained in Test Requirement C.2.3.1.a, the assessor shall examine evidence to confirm that authorization checks are performed each time users request access to a function or resource exposed (or potentially exposed) through Internet-accessible interfaces to verify they are authorized for the function, resource, and type of access requested.	**R1** Describe how the software verifies whether users are authorized to access functions or resources exposed through APIs or other interfaces.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.3.2.b The assessor shall examine evidence and test the software to confirm that access control rules are enforced each time a user attempts to access a function or resource exposed (or potentially exposed) through Internet-accessible interfaces.	**R1** Identify each of the software tests performed, including the tool(s) or method(s) used and the scope of each test, to confirm that access control rules are enforced each time a user attempts to access the functions and resources exposed through APIs or other interfaces.			
	R2 Describe what the assessor observed in the evidence obtained that confirms that access control rules are enforced each time a user attempts to access the functions and resources exposed through APIs or other interfaces.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.2.3.3 Access control decisions are enforced within a secure area of the software architecture.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.2.3.3.a The assessor shall examine evidence to identify where in the software architecture authorization and access control decisions are enforced.	**R1** Identify the evidence obtained that details the locations within the software architecture where authorization and access control decisions are enforced.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.3.3.b The assessor shall examine evidence to confirm that all access control decisions are enforced within a secure area of the software architecture.	**R1** Describe what the assessor observed in the evidence obtained that confirms all authorization and access control decisions are enforced within a secure area of the software architecture.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.2.3.3.c The assessor shall examine evidence and test the software to confirm that client-side or browser-based functions, scripts, and data are never solely relied upon for access control purposes.	**R1** Indicate whether client-side or browser-based functions, scripts, or data are relied upon for access control purposes.			
	R2 If R1 is "Yes," then describe how the software uses these functions, scripts, or data for access control.			
	R3 If R1 is "Yes," then describe the methods implemented to ensure the compromise of client-side or browser-based functions, scripts, or data cannot be used to manipulate access control decisions.			
	R4 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective C.3: Web Software Attack Mitigation Software security controls are implemented to mitigate common attacks on web applications.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.3.1 The software enforces or otherwise supports the use of the latest HTTP Security Headers to protect Internet accessible interfaces from attacks.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.3.1.a The assessor shall examine evidence to confirm the software supports the use of the latest HTTP Security Headers, and to determine the options available and how such settings are configured.	**R1** Identify the evidence obtained that details the primary set of HTTP Security Headers and configuration options that are supported by the software.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.1.b Where HTTP Security Headers are configured and controlled by the software provider, the assessor shall examine evidence to confirm that the software is configured to use the latest available HTTP Security Headers and that the configuration settings are reasonable and justified.	**R1** Indicate whether HTTP Security Headers are configured and controlled by the assessed software or entity.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe what the assessor observed in the evidence obtained that confirms the software is configured to use the latest available HTTP Security Headers.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.1.c Where user input or interaction is required to configure HTTP Security Headers, the assessor shall examine evidence to confirm that guidance is made available to stakeholders in accordance with Control Objective 12.1 that describes the HTTP Security Headers supported by the software and how to configure such settings.	**R1** Indicate whether user input or interaction is required to configure HTTP Security Headers.	☐ Yes ☐ No		
	R2 If R2 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring the software to use HTTP Security Headers securely.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.3.2 Input data from untrusted sources is never trusted and software security controls are implemented to mitigate the exploitation of vulnerabilities through the manipulation of input data.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.3.2.a Using information obtained in Test Requirement C.2.1.a, the assessor shall examine evidence to identify all interfaces that accept data input from untrusted sources.	**R1** Identify the evidence obtained that details all APIs and other interfaces that accept input data from untrusted sources.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.2.b Where the software accepts input from untrusted sources, the assessor shall examine evidence to identify the data format(s) expected by the software for each input field and the parsers and interpreters involved in processing the input data.	**R1** Identify the evidence obtained that details the data format(s) expected for each of the input fields identified in Test Requirement C.3.2.a and the parsers or interpreters involved in the processing of the input data.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.2.c Using information obtained in Test Requirement 4.1.a in the Core Requirements section, the assessor shall examine evidence to determine whether attacks that target all such parsers and interpreters are acknowledged in the threat model.	**R1** Describe what the assessor observed in the evidence obtained that confirms attacks on the parsers and interpreters identified in Test Requirement C.3.2.b are covered in the software vendor's threat analysis.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.2.d Where such attacks are acknowledged and using information obtained in Test Requirement 4.2.a in the Core Requirements section, the assessor shall examine evidence to confirm that software security controls are defined and implemented to mitigate attacks that attempt to exploit vulnerabilities through the manipulation of input data.	**R1** Describe what the assessor observed in the evidence obtained that confirms that software security controls are implemented to mitigate attempts to exploit vulnerabilities in these parsers and interpreters through the manipulation of input data.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.3.2.e Where the implementation of software security controls is configurable or otherwise requires user input or interaction, the assessor shall examine evidence to confirm that guidance is made available to stakeholders in accordance with Control Objective 12.1 that describes how to properly configure such security controls.	**R1** Indicate whether any of the security controls described in Test Requirement C.3.2.d are user configurable.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring these security controls securely.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.2.1 Industry-standard methods are used to protect software inputs from attacks that attempt to exploit vulnerabilities through the manipulation of input data.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.3.2.1.a Using information obtained in Test Requirement 4.2.a in the Core Requirements section, the assessor shall examine evidence to identify all software security controls implemented to mitigate attacks that attempt to exploit vulnerabilities through the manipulation of input data.	**R1** Describe the methods relied upon by the software to mitigate attempts to exploit vulnerabilities in parsers and interpreters through the manipulation of input data.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.2.1.b The assessor shall examine evidence to confirm that the methods implemented to protect against such attacks use industry-standard mechanisms and/or techniques that are: • Provided by well-known and industry-accepted third-party suppliers; or • Designed and implemented in accordance with applicable industry standards or best practices.	**R1** Describe what the assessor observed in the evidence obtained that confirms that the methods implemented to protect against such attacks use industry-standard mechanisms or techniques.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.3.2.1.c The assessor shall examine evidence and test the software to confirm that the implemented methods: • Are implemented correctly in accordance with available guidance, and • Do not expose any vulnerabilities.	**R1** Describe what the assessor observed in the evidence obtained that confirms the methods implemented to protect against attempts to exploit vulnerabilities in parsers and interpreters through the manipulation of input data are implemented correctly and do not expose vulnerabilities.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.2.2 Parsers and interpreters are configured with the most restrictive configuration feasible.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.3.2.2.a Using information obtained in Test Requirement C.3.2.b, the assessor shall examine evidence to identify the configurations for each parser or interpreter used to process untrusted input data.	**R1** Identify the evidence obtained that details the (default) configurations for each parser or interpreter used to process untrusted input data.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.2.2.b For each of the parsers/interpreters and the configurations identified, the assessor shall examine evidence to confirm that parsers and interpreters are configured with the most restrictive set of capabilities feasible and that the settings are justified and reasonable. Where certain parser/interpreter features cannot be configured securely, the assessor shall examine evidence to confirm that other methods are implemented to mitigate the lack of secure settings and to further protect against the execution of malicious commands.	**R1** Describe what the assessor observed in the evidence obtained that confirms that parsers and interpreters are configured with the most restrictive set of capabilities feasible.			
	R2 Describe the methods implemented to mitigate the exploitation of exposed vulnerabilities in parsers or interpreters.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.3.3 Software security controls are implemented to protect software interfaces from resource starvation attacks.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.3.3.a Using information obtained in Test Requirements C.2.1.a and C.2.2, the assessor shall examine evidence to identify all Internet accessible interfaces and the functions and resources exposed (or potentially exposed) through those interfaces to identify where such interfaces, functions, and resources may be susceptible to resource starvation attacks.	**R1** Identify the evidence obtained that details the interfaces, functions, and resources potentially susceptible to resource starvation attacks.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.3.b Where such interfaces, functions, and resources are potentially susceptible to resource starvation attacks, the assessor shall examine evidence to confirm that: • The threat of such attacks is documented in accordance with Control Objective 4.1, and • Software security controls to mitigate such attacks are documented and implemented in accordance with Control Objective 4.2.	**R1** Describe what the assessor observed in the evidence obtained that confirms that the threats related to resource starvation attacks are documented in the software vendor's threat analysis.			
	R2 Describe the security controls implemented to protect against resource starvation attacks.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.3.c The assessor shall examine evidence to confirm that the software security controls implemented to mitigate resource starvation and other similar attacks on Internet accessible interfaces are designed and implemented in accordance with applicable industry standards and best practices.	**R1** Describe what the assessor observed in the evidence obtained that confirms that software security controls implemented to protect against resource starvation attacks are aligned with industry standards and best practices regarding such protections.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.3.3.d Where the implementation of software security controls is user configurable or otherwise requires user input or interaction, the assessor shall examine evidence to confirm that guidance is made available to stakeholders in accordance with Control Objective 12.1 that describes how to configure such mechanisms.	**R1** Indicate whether software security controls to protect against resource starvation attacks are user configurable.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring such methods.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.4 Software security controls are implemented to protect Internet accessible interfaces from malicious file content.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.3.4.a Using information obtained in Test Requirement C.2.1.a, the assessor shall examine evidence to identify all Internet accessible interfaces that accept file uploads and the file types permitted.	**R1** Identify the evidence obtained that details the software interfaces that accept file uploads, and file types supported.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.4.b Where the software accepts file uploads over Internet accessible interfaces, the assessor shall examine evidence to confirm that: • The threat of attacks on file upload mechanisms is documented in accordance with Control Objective 4.1, and • Software security controls to mitigate such attacks are documented and implemented in accordance with Control Objective 4.2.	**R1** Describe what the assessor observed in the evidence obtained that confirms that threats to interfaces that accept file uploads are documented.			
	R2 Describe the software security controls implemented to mitigate common attacks that target file upload mechanisms.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
C.3.4.c The assessor shall examine evidence to confirm that the software security controls implemented to mitigate attacks on file upload mechanisms are implemented in accordance with applicable industry standards and best practices.	**R1** Describe what the assessor observed in the evidence obtained that confirms that software security controls implemented to mitigate attacks on file upload mechanisms are designed in accordance with applicable industry-standard methods.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
C.3.4.d The assessor shall examine evidence to confirm that the software security controls implemented to mitigate attacks on file upload mechanisms include methods to restrict the file types permitted by the file upload mechanisms.	**R1** Describe the methods implemented by the software to restrict the types of files permitted and the types of files permitted by default.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
C.3.4.e The assessor shall examine evidence to confirm that the software security controls implemented to mitigate attacks on file upload mechanisms include methods to restrict the maximum number and size of files permitted for upload.	**R1** Describe the methods and/or mechanisms implemented by the software to mitigate attacks that attempt to overwhelm or exploit file parsing mechanisms using excessive file sizes or excessive file uploads.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
C.3.4.f The assessor shall examine evidence to confirm that the software security controls implemented to mitigate attacks on file upload mechanisms account for the use of complex or compressed file formats that are often used to overwhelm or otherwise exploit file-parsing mechanisms.	**R1** Describe the methods and/or mechanisms implemented by the software to mitigate attacks that attempt to overwhelm or exploit file-parsing mechanisms using complex or compressed file formats.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.3.4.g The assessor shall examine evidence to confirm that the software security controls implemented to mitigate attacks on file upload mechanisms include methods that store uploaded files outside of the webroot and assign those files read-only permissions.	**R1** Describe the methods and/or mechanisms implemented by the software to mitigate attacks that attempt to remotely execute malicious code through direct calls to uploaded files.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.4.h The assessor shall examine evidence to confirm that the use of file-parsing mechanisms does not rely on file names or file extensions for security purposes.	**R1** Describe the methods and/or mechanisms implemented by the software to mitigate attacks that attempt to trick the software into interpreting files of one type as another type.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.4.i Where the implementation of software security controls is user configurable or otherwise requires user input or interaction, the assessor shall examine evidence to confirm that guidance is made available to stakeholders in accordance with Control Objective 12.1 that describes how to configure such mechanisms.	**R1** Indicate whether any of the software security controls implemented to protect against attacks on file parsing mechanisms are user configurable or require user input or interaction to be enabled.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring applicable security controls.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.5 Software security controls are implemented to protect Internet accessible interfaces from hostile object creation and data tampering.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.3.5.a Using information obtained in Test Requirements C.2.1.a and C.2.2, the assessor shall examine evidence to identify all software functions exposed through Internet accessible interfaces that accept and process data objects as inputs.	**R1** Identify the evidence obtained that details the software interfaces and functions that accept and process data objects as inputs.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
C.3.5.b Where the software accepts and processes data objects as inputs, the assessor shall examine evidence to confirm that: • The threat of hostile object creation and data tampering attacks is documented in accordance with Control Objective 4.1, and • Software security controls to mitigate such attacks are documented and implemented in accordance with Control Objective 4.2.	**R1** Describe what the assessor observed in the evidence obtained that confirms that threats to interfaces that accept and process data objects as inputs are documented.	
	R2 Describe the software security controls implemented to mitigate common attacks on these types of interfaces and functions.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
C.3.5.c The assessor shall examine evidence to confirm that the software security controls implemented to mitigate hostile object creation and data tampering attacks are implemented in accordance with applicable industry standards and best practices.	**R1** Describe what the assessor observed in the evidence obtained that confirms that software security controls implemented to mitigate hostile object creation and data tampering attacks are designed in accordance with applicable industry-standard methods.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
C.3.5.d The assessor shall examine evidence to confirm that the software security controls implemented to mitigate hostile object creation and data tampering attacks include methods that restrict the file formats permitted by file-parsing mechanisms.	**R1** Describe the methods implemented by the software to restrict the file formats permitted by file-parsing mechanisms.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
C.3.5.e The assessor shall examine evidence to confirm that the use of file-parsing mechanisms does not rely on file names or file extensions for security purposes.	**R1** Describe how the software handles files that have been renamed or restructured to force the software to parse the file contents using unintended file-parsing mechanisms or interpreters.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
C.3.5.f The assessor shall examine evidence to confirm that the use of file-parsing mechanisms does not expose other vulnerabilities.	**R1** Describe what the assessor observed in the evidence obtained that confirms that file-parsing mechanisms do not contain or otherwise expose vulnerabilities.	
	R2 Describe any other assessment activities performed and/or findings for this test requirement.	
C.3.5.g Where the software accepts serialized objects as inputs, the assessor shall examine evidence to confirm that software security controls are implemented to protect against deserialization attacks and that such security controls adhere to applicable industry standards and best practices.	**R1** Indicate whether the software accepts serialized objects as inputs.	☐ Yes ☐ No
	R2 If R2 is "Yes," then describe the software security controls implemented to protect against deserialization attacks.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	
C.3.5.h Where the software security controls implemented to protect against hostile object creation and data tampering are user configurable or otherwise require user input or interaction, the assessor shall examine evidence to confirm that guidance is made available to stakeholders in accordance with Control Objective 12.1 that describes how to configure such mechanisms.	**R1** Indicate whether any of the software security controls are user configurable or require user input or interaction to be enabled.	☐ Yes ☐ No
	R2 If R2 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring applicable security controls.	
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
C.3.6 Software security controls are implemented to protect Internet accessible interfaces from attacks that exploit multi-origin resource sharing.		**In Place** ☐	**Not in Place** ☐	**N/A** ☐
C.3.6.a The assessor shall examine evidence to determine if and/or how the software supports cross-origin access to Internet accessible interfaces, and to confirm that access to software APIs and resources from browser-based scripts is disabled by default.	**R1** Indicate whether the software supports cross-origin access to software interfaces.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then describe the mechanisms implemented to restrict access to API endpoints and resources from browser-based scripts.			
	R3 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.6.b Where cross-origin access is enabled, the assessor shall examine evidence to confirm that the reasons for enabling cross-origin access are reasonable and justified, and that access is restricted to the minimum number of origins feasible.	**R1** Describe what the assessor observed in the evidence obtained that confirms access is restricted to the minimum number of origins feasible.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.6.c The assessor shall test the software to confirm that the claims made by the assessed entity regarding cross-origin access are valid. At a minimum, testing is expected to include functional testing using forensic tools/techniques.	**R1** Describe each of the tests performed, including the tool(s) or method(s) used and the scope of each test to validate the findings in Test Requirement C.3.6.b.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.3.6.d Where the disabling or restricting cross-origin access to software APIs requires user input or interaction, the assessor shall examine evidence to confirm that appropriate guidance on this process is provided to stakeholders in accordance with Control Objective 12.1.	**R1** Indicate whether any software security controls implemented to restrict cross-origin access to software interfaces are user configurable or require user input or interaction to be enabled.	☐ Yes ☐ No		
	R2 If R1 is "Yes," then identify the evidence obtained that details the software vendor's guidance on configuring applicable security controls.			

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings
	R3 Describe any other assessment activities performed and/or findings for this test requirement.	

Control Objectives / Test Requirements	Reporting Instructions	Assessor's Findings		
Control Objective C.4: Web Software Communications Sensitive data transmissions are secured in accordance with Control Objective 6.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.4.1 Sensitive data transmissions are encrypted in accordance with Control Objectives 6.2 and 6.3.		**In Place**	**Not in Place**	**N/A**
		☐	☐	☐
C.4.1.a Using information obtained in Test Requirement 6.2.a, the assessor shall examine evidence to determine how communications are handled by the software, including those between separate systems in the overall software architecture.	**R1** Identify the evidence obtained that details the full architecture of the assesses software, including all components that reside both within and outside the physical execution environment.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			
C.4.1.b Where the software allows or otherwise supports the transmission of sensitive data between users and systems in different security contexts, the assessor shall examine evidence to confirm that all such communications are encrypted using strong cryptography in accordance with Control Objectives 6.2 and 6.3.	**R1** Describe what the assessor observed in the evidence obtained that confirms that communications between components in different security contexts is encrypted using strong cryptography in accordance with Control Objective 6.2 and 6.3.			
	R2 Describe any other assessment activities performed and/or findings for this test requirement.			

Appendix A Additional Information Worksheet

If the Reporting Details column in the Findings and Observations section does not possess enough space for a particular control objective and test requirement, use this Appendix to include the additional information. Record in the Assessor's Findings column for that test requirement that additional information is recorded in Appendix A.

Control Objective	Test Requirement	Additional Information
Ex: 3.2	*3.2.b*	*A table containing an inventory of all open-source components used by the vendor's software is attached to this ROV.*

Appendix B Testing Environment Configuration for Secure Software Assessments

The assessor must confirm that the environment used to conduct the Secure Software Assessment was configured in accordance with Section 4.6.1 of the *Secure Software Program Guide*. This confirmation must be submitted to PCI SSC with the completed *Report on Validation (ROV)*.

B.1 Secure Software Assessor Company Testing Environment	
Describe the Secure Software Assessor Company's Test Environment(s) used by the Assessor for this assessment (adding rows as needed).	
Identify the organization(s) responsible for configuring the lab/test environment used for this assessment (select all that apply):	☐ Secure Software Assessor Company ☐ Software Vendor ☐ Third Party (please specify):
Identify the address(es) and/or location(s) of the lab/test environment(s) used for this assessment. If the lab/test environment is virtual, then identify the platform(s) used and the geographic region(s) and/or availability zone(s) where the lab/test environment resides.	
Describe each of the lab/test environments used for this assessment including how they are configured. Where more than one lab/test environment is used, be clear which lab/test environment is being described and who was responsible for configuring the test environment.	
Describe methods implemented to prevent test environment tampering to ensure the integrity of the software assessment.	

B.2 Confirmation of Testing Environment Used	
Indicate whether the Secure Software Assessor Company's Testing Environment(s) described in Section B.1 adhere(s) to the requirements specified in Section 4.6.1 of the *Secure Software Program Guide*. If "No," then provide reasons why the Secure Software Assessor Company Test Environment is not capable of properly and fully testing all functions of the Payment Software and describe the alternative environment(s) used in the field below:	☐ Yes ☐ No

B.3 Confirmation of Testing Environment Configuration	
Confirm the following for each of the Secure Software Assessor Company's Test Environments used for this assessment: **Note:** If any of the questions below are determined to be "not applicable," select "No" for the response and provide a detailed explanation as to why the questions are not applicable in B.4 where prompted.	
All testing of the Payment Software occurred in a pristine computing environment, free from potentially conflicting applications, network traffic, security and/or access controls, software versions, and artifacts or "orphaned" components left behind from other software installations.	☐ Yes ☐ No
The testing environment simulated the "real world" use of the Payment Software.	☐ Yes ☐ No
The Payment Software was installed and/or configured in accordance with the Vendor's installation manual, training materials, and Security Guidance.	☐ Yes ☐ No
All implementations of the Payment Software, including region/country specific versions, intended to be listed on the PCI SSC website were tested.	☐ Yes ☐ No
All Payment Software versions and platforms, including all necessary system components and dependencies, intended to be listed on the PCI SSC website were tested.	☐ Yes ☐ No
All critical payment software functionalities were tested.	☐ Yes ☐ No
Production data (i.e., live PAN) was not used for testing.	☐ Yes ☐ No
All authorization and/or settlement functions were tested and the output from those functions examined.	☐ Yes ☐ No
All functions of the Payment Software were simulated and validated.	☐ Yes ☐ No
The testing environment was configured in a manner to support the exploitation of software vulnerabilities in the Payment Software (i.e., the configuration of the testing environment did not prevent software vulnerabilities from being tested).	☐ Yes ☐ No

B.4 Attestation of Test Environment Validation	
Provide the name of the Secure Software Assessor who attests that all items in tables B.1 through B.3 were validated, and all details are consistent with the details in the rest of the Report on Validation.	
If any of the items in B.3 were marked as "No," describe why those items could not be confirmed and why the circumstances surrounding the lack of confirmation are acceptable.	
Specify any other details or comments related to the testing environment that the Secure Software Assessor would like to note.	