Payment Card Industry (PCI)
Software Security Framework

Secure Software Template for Report on Validation

Version 1.1

April 2021

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.

Table of Contents

Introduction to the PCI Secure Software ROV Reporting Template

This document, the *PCI Software Security Framework – Secure Software Template for Report on Validation* (hereafter referred to as the *Secure Software ROV Reporting Template*) is for use with the *PCI Software Security Framework – Secure Software Requirements and Assessment Procedures* (PCI Secure Software Standard) Version 1.1 and is the mandatory template for Secure Software Assessors completing a Secure Software Assessment. The Secure Software ROV Reporting 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.

This Reporting Template is mandatory for all Secure Software Assessment report submissions to PCI SSC.

Tables have been included in this template to assist with the reporting process for certain lists and other information as appropriate. You can modify the tables in this template to increase or decrease the number of rows or to change column width. The assessor may add appendices to include relevant information that is not addressed by the current organization. However, the assessor must not remove any details from the tables provided in this document. Customization is acceptable, such as the addition of company logos, but should be limited to the title page and the headers for the remainder of the document.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as they complete reporting, but also provide context for the report recipient(s). The inclusion of additional text or sections is permitted within reason, as noted above.

A Secure Software Assessment involves thorough testing and assessment activities from which the assessor generates detailed work papers for each control objective and its associated test requirements. These work papers contain comprehensive 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) is effectively a summary of evidence derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached and justified. At a high level, the Secure Software ROV is a comprehensive summary of testing activities performed and information 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.

Use this template in conjunction with the appropriate versions of the following PCI Software Security Framework documents, which are available on the PCI SSC website at https://www.pcisecuritystandards.org.

- *Software Security Framework – Secure Software Requirements and Assessment Procedures*
- *Software Security Framework – Secure Software Program Guide*
- *Software Security Framework – Secure Software Attestation of Validation*
- *Software Security Framework – Glossary of Terms, Abbreviations, and Acronyms*
- *Software Security Framework – Qualification Requirements for Assessors*

Secure Software ROV Reporting Template Sections

The Secure Software ROV Reporting Template includes the following sections:

1. Contact Information and Report Summary
2. Software Overview
3. Assessment Overview
4. Assessor Company Attestations
5. Findings and Observations

The Secure Software ROV Reporting Template also includes the following Appendices:

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

All numbered sections must be thoroughly and accurately completed. The Secure Software ROV Reporting 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 the testing procedure within a description is discouraged, as it does not add any level of assurance to the narrative. Use of template language for summaries and descriptions is discouraged and details should be specifically relevant to the assessed software.

Documenting the Assessment Findings and Observations

Within the Findings and Observations section of the *Secure Software ROV Reporting Template* is where the detailed results of the software assessment are documented. In this section, an effort was made to efficiently use space and provide a snapshot view of assessment results (Summary of Assessment Results) ahead of the detailed reporting that is to be specified in the "Reporting Details: Assessor's Response" column. An example layout of the Findings and Observations section is provided in Table 1.

Table 1. Findings and Observations

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
1.1 Detailed Control Objective Summary			**In Place**	**N/A**	**Not in Place**
			☐	☐	☐
1.1.a Test Requirement	Reporting Instruction				
	Reporting Instruction				

For the Summary of Assessment Findings, there are three results possible—In Place, Not Applicable (N/A), and Not in Place. 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.
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 organization or their software development practices. All "N/A" responses require reporting on the testing performed to confirm the "N/A" status. Note that a "N/A" response still requires a detailed description explaining how it was determined that the control objective does not apply.

Understanding the Reporting Instructions

In addition to specifying whether a control objective is "In Place," "N/A," or "Not in Place," under the Summary of Assessment Findings column, the Secure Software Assessor must also document their findings for each test requirement under the Reporting Details column within the Findings and Observations section. One or more reporting instructions are provided for each test requirement. Responses are required for all reporting instructions except where explicitly indicated within the 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 is 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 documentation and evidence examined that outlines 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.*
Summarize	Summarize how the software prevents sensitive data from being processed until initialization is complete.	The response would provide a high-level overview of a security control, process, mechanism, or tool that is implemented or used by the vendor to satisfy a control objective. For example, summarizing a security control or protection mechanism would include information about what is implemented, what it does, and how it meets its purpose.

While it is expected that a Secure Software Assessor will perform all reporting instructions identified for each test requirement, it may also be possible for a control objective to be validated using different or additional assessment procedures. In such cases, the Secure Software Assessor should describe in the Reporting Details: Assessor's Response column within the Findings and Observations section why assessment procedures that differ from the test requirements identified in the Secure Software Standard were used and describe how those assessment procedures provide at least the same level of assurance that would have been achieved using the stated 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 and information 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, and components 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 either "dd/mmm/yyyy" or "mmm/dd/yyyy" format, and using the same 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 used in section 3.7 of the *Secure Software ROV Reporting Template* rather than list out the items from the sample within the individual reporting instruction response. If sampling is not used, then the evidence that was evaluated must still be identified in the Findings and Observations section and recorded using Sample Set Reference numbers in section 3.8.

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 Reporting Details: Assessor Response column within the 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 4.5.1 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.*

Template for PCI Secure Software Report on Validation

This template is to be used for creating a Secure Software Report on Validation. Content and format of the ROV are defined as follows:

1. Contact Information and Report Summary

1.1 Contact Information			
Software Vendor Contact Information			
Company name:		Company contact name:	
Contact e-mail address:		Contact phone number:	
Secure Software Assessor Contact Information			
Assessor company name:		Assessor name:	
Assessor e-mail:		Assessor phone number:	
Confirmation that internal QA was fully performed on the entire submission per requirements in the relevant program documentation.	☐ Yes ☐ No *Note: If "No," this is not in accordance with PCI Program requirements.*	QA reviewer name:	
		QA reviewer phone number:	
		QA reviewer e-mail address:	

1.2 Date and Timeframe of Assessment	
Date of report: ***Note**: This date must be shown as the "Secure Software ROV Completion Date" in the Secure Software AOV.*	
Timeframe of assessment (start date to completion date):	
Identify date(s) spent onsite at the Software Vendor, if applicable:	
Describe how time was spent onsite at the Software Vendor, how time was spent performing remote assessment activities, and how time was spent on validation of remediation activities: ***Note**: Provide range of dates for each activity.*	

1.3 PCI Secure Software Version	
Version of the PCI Secure Software Standard used for this assessment:	

2. Software Overview

2.1 Software Details			
Software name tested:		Software version tested (wildcards not permitted):	
Is the software already listed on the PCI SSC List of Validated Payment Software?	☐ Yes ☐ No	If "yes," provide the Validated Payment Software name and PCI Identifier:	
Payment Software Type for this software (Please refer to Section A.2 of the *Secure Software Program Guide* for a detailed explanation of software types):			
☐ (01) POS Suite/General ☐ (02) Payment Middleware ☐ (03) Payment Gateway/Switch	☐ (04) Payment Back Office ☐ (05) POS Admin ☐ (06) POS Specialized	☐ (07) POS Kiosk ☐ (08) POS Face-to-Face/POI ☐ (09) Shopping Cart / Store Front	☐ (10) Card-Not-Present ☐ (11) Automated Fuel Dispenser ☐ (12) Payment Component
Describe the software function and purpose (for example, the types of transactions performed, the specific payment acceptance channels supported, etc.):			
Describe how the software is sold, distributed, or licensed to third parties (for example, licensed as software-as-a-service, stand-alone application, etc.):			
Describe how the software is designed (for example, as a standalone application, as a component or library, or as part of a suite of applications)			
Describe a typical implementation of the software (for example, how it is configured in the execution environment or how it typically interacts with other systems or components).			

2.2 Software Versioning	
Describe how the software vendor indicates changes to their payment software via version numbers and/or their versioning methodology:	
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): ***Note**: Wildcards are not permitted*	
Describe the hierarchy of the elements, including what each element represents in the version scheme:	
Other important details regarding the versioning scheme (where necessary):	

2.3 Hardware Platform Requirements and/or Dependencies	
Does the assessed payment software rely on any specific third-party or proprietary hardware platforms for its intended execution?	☐ Yes ☐ No
If "yes," identify and list all hardware the assessed payment software relies upon for its operation:	

Device Make / Manufacturer	***Device Model Name / Number***	***Device Version** (wildcards permitted)*	***Device Description** (e.g., device type, function, etc.)*
Example: Acme, Inc.	*Acme POS*	*v1.x*	*Integrated POS, secure card reader and pin-entry device.*

2.4 Software Platform Requirements and/or Dependencies			
Does the assessed payment software rely on any specific third-party or proprietary software platforms for its intended execution?	☐ Yes ☐ No		
If "yes," identify and list all software the assessed payment software relies upon for its operation:			
Software Vendor / Owner	***Software Name***	***Software Version*** *(wildcards permitted)*	***Software Description*** *(e.g., type, function, etc.)*
Example: Acme, Inc.	*Acme E-commerce Server*	*v2.x*	*Web/application server*

2.5 Other Required Software Components			
Does the assessed payment software rely on any other third-party or proprietary software, APIs, or components to provide its intended functionality?	☐ Yes ☐ No		
If "yes," identify and list all software, APIs, and components the assessed payment software relies upon to provide the full scope of its intended functionality:			
Software Vendor / Owner	***Software Name***	***Software Version*** *(wildcards permitted)*	***Software Description*** *(e.g., type, function, etc.)*
Example: Acme, Inc.	*Acme Crypto Library*	*v3.x*	*Suite of cryptographic libraries used for authentication and data protection.*

2.6 Sensitive Data Overview

Identify the types of sensitive data stored, processed and/or transmitted by the software and describe how each is handled:

***Note**: Additional rows may be added to accommodate additional sensitive data types. Refer to the Software Security Framework – Glossary of Terms, Abbreviations, and Acronyms for more information on how Sensitive Data is defined.*

Sensitive Data Store *(file [name], table [name], etc.)*	***Sensitive Data Type*** *(e.g., Account Data, authentication credentials, etc.)*	***Description of Sensitive Data Elements*** *(e.g., PAN/SAD, username/password, etc.)*	***Summary of How the Sensitive Data is Handled*** *(e.g., stored, processed, transmitted, etc.)*	***Summary of How the Sensitive Data is Protected*** *(e.g., encrypted during transmission, hashed during storage, etc.)*

2.7 Overview of Sensitive Functions Provided

Identify the sensitive functions provided by the software and describe how each is protected:

***Note**: Additional rows may be added to accommodate additional sensitive data types. Refer to the Software Security Framework – Glossary of Terms, Abbreviations, and Acronyms for more information on how Sensitive Functions are defined.*

Sensitive Function Type *(e.g., user authentication, data encryption, encryption key management, etc.)*	***Associated Sensitive Data Types*** *(e.g., account data, authentication credentials, etc.)*	***Summary of How Sensitive Functions are Protected*** *(e.g., access control mechanisms, integrity checks, etc.)*

2.8 Overview of Sensitive Resources Used

Identify the sensitive resources used by the software and describe how interactions with them are secured:

Sensitive Resource Name *(e.g., LDAP, libcrypto, keychain, etc.)*	***Associated Sensitive Function*** *(user authentication, data encryption, encryption key management, etc.)*	***Source / Provider*** *(The entity that maintains the code e.g., Microsoft, Verifone, Ingenico, etc.)*	***Summary of How Interactions are Secured*** *(e.g., mutual authentication, access control, obfuscation, etc.)*

2.9 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 data flows, including any output to hardcopy, paper, or other external media. The sensitive data describe here should be consistent with the information provided in Sections 2.6 through 2.8.*

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 Scope	
Identify the requirement modules within the *Secure Software Standard* the software was assessed to: ***Note**: if the payment software stores, processes, or transmits Account Data, the software must be assessed to both the Core Requirements and the Account Data Protection module.*	☐ Core Requirements ☐ Module A – Account Data Protection Requirements ☐ Module B – Terminal Software Requirements

3.2 Hardware Platforms and Components Tested				
Identify/describe all hardware platforms and components the assessed payment software was tested on/with during the assessment:				
Device Make / Manufacturer	***Device Model Name / Number***	***Device PCI Approval Number** (if applicable)*	***Device Hardware and/or Firmware Version** (no wildcards)*	***Device Description** (e.g., device type, function, etc.)*

3.3 Software Platforms and Components Tested

Identify/describe all software platforms (including operating systems) and components the assessed payment software was tested on/with during the assessment:

Software Vendor / Owner	***Software Name***	***Software Version*** *(no wildcards)*	***Software Description*** *(e.g., type, function, etc.)*

3.4 System Configurations Tested

Describe each unique combination of hardware and software (including those identified in Section 3.2 and 3.3) used to validate the payment software, as well as other important details of the testing environment (for example, how the various platforms and components are configured to communicate with one another, whether any of the hardware/software components were virtualized, etc.).

Describe who provided the environment(s) where the software was tested (e.g., the Secure Software Assessor Company, the software vendor, a third-party, a combination of two/all three, etc.):

3.5 Documentation / Evidence Reviewed

Identify and list the documents, materials and other evidence examined during testing:

Reference Number	***Document Name*** *(including version, if applicable)*	***Document Description / Purpose***	***Document Generation Method***	***Document Date*** *(date last updated)*
Doc-1			☐ Manual ☐ Automated	
Doc-2			☐ Manual ☐ Automated	
Doc-3			☐ Manual ☐ Automated	
Doc-4			☐ Manual ☐ Automated	
Doc-5			☐ Manual ☐ Automated	

3.6 Individuals Interviewed

Identify and list the individuals interviewed during testing:

Reference Number	***Individual's Name***	***Role / Job Title***	***Organization***	***Summary of Topics Covered*** *(high-level summary only)*
Int-1				
Int-2				
Int-3				
Int-4				
Int-5				

3.7 Software Testing Performed			
Identify and describe each of the software tests performed during testing and the scope of each test:			
Reference Number	***Test Type / Description*** *(e.g., type of test performed, forensic tools used, etc.)*	***Test Scope*** *(e.g., software components and/or features evaluated)*	***Control Objectives Covered*** *(No generic references)*
Test-1	Manual source code review	User authentication module	5.1, 5.2, 5.3
Test-2			
Test-3			
Test-4			
Test-5			

3.8 Sampling Methodology and Sample Sets Used

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.)

Identify and list all the sample sets used during testing:

***Note**: When a reporting instruction asks to identify a sample, the Secure Software Assessor must identify the items sampled (for example, as "Set-1") in the table below and then specify the corresponding sample set reference number in the Assessor Response field next to the applicable reporting instruction in the Findings and Observations section. The existing rows representing pre-defined sample sets must not be deleted. However, the assessor may add rows to this table as needed to accommodate additional sample sets.*

Where sampling is used (or where instructed), samples must be representative of the total population. The sample size must be sufficiently large and diverse to provide assurance that the selected sample accurately reflects the overall population, and that any resultant findings based on a sample are an accurate representation of the whole. In all instances where a Secure Software Assessors finding is based on a representative sample rather than the complete set of applicable items, the assessor should explicitly record this fact, identify the items chosen as samples for the testing, and explain the sampling methodology used.

Reference Number	***Sample Type / Description*** *(e.g., systems, software updates, etc.)*	***Listing of All Items in Sample Set*** *(unique system identifiers, software versions, etc.)*	***Total Sampled***	***Total Population***	***Assessor Justification*** *(for sample size chosen)*
Set-1	Software updates sampled in 11.1.b				
Set-2					
Set-3					

4. Assessor Company Attestations

A duly authorized representative of the Assessor Company hereby confirms the following:

4.1 Attestation of Independence

- This assessment was conducted strictly in accordance with all applicable requirements set forth in Section 2.2 of the *Software Security Framework Qualification Requirements for Assessors*, including but not limited to the requirements therein regarding independence, professional judgment, integrity, objectivity, impartiality, and professional skepticism;
- This Report on Validation accurately identifies, describes, represents, and characterizes all the 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 in the course of performing the assessment; and
- 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.

4.2 Attestation of Software Eligibility

- To the best of their knowledge, the assessed payment software is eligible for validation in accordance with the *Secure Software Program Guide*:

4.3 Attestation of Scoping Accuracy

- To the best of their knowledge, all information pertaining to the assessed payment software is accurately represented in "Section 2: Software Details."

4.4 Attestation of Sampling

- To the best of their knowledge, all sample sets used for this Secure Software Assessment are accurately represented in "Section 3.8: Sample Sets Used."

Signature of Authorized Assessor Employee ↑	*Date:*
Assessor Employee Name:	*Assessor Company Name:*
***Note**: This section must be printed and signed manually, or digitally signed using a legally recognized electronic signature.*	

5. Findings and Observations

Minimizing the Attack Surface

The attack surface of the software is minimized. Confidentiality and integrity of all software critical assets are protected, and all unnecessary features and functions are removed or disabled.

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 1: Critical Asset Identification All software critical assets are identified					
1.1 All sensitive data stored, processed, or transmitted by the software is identified.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
1.1.a The assessor shall examine vendor evidence to confirm that it 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).	**Identify** the documentation and evidence examined that identifies and describes all sensitive data that is stored, processed, and transmitted by the software.				
1.1.b For each item of sensitive data, the assessor shall examine vendor evidence to confirm that evidence describes where this data is stored, and the applicable security controls implemented to protect the data. This includes 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).	For each item of sensitive data identified in 1.1.a, **identify** the documentation and evidence examined that describes where each item of sensitive data is stored (including storage in temporary locations, semi-permanent locations, and non-volatile locations), and the security controls implemented to protect the sensitive data.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
1.1.c The assessor shall examine vendor evidence and test the software to identify where the implementation enforces storage within a specific location or form factor (such as with an embedded system that is only capable of local storage). The assessor shall confirm that the data for all of these is supported by the vendor evidence.	**Identify** the documentation and evidence examined that describes where the software implementation enforces storage of sensitive data within a specific location or form factor.		
	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.		
	Describe any discrepancies that were found between the information obtained through documentation and evidence review and information obtained through software testing.		
1.1.d The assessor shall examine vendor evidence and test the software to validate the information provided by the vendor in Test Requirement 1.1.a. ***Note:*** *The assessor may require and rely on assistance from the software vendor to complete this test requirement (such as through access to a dedicated test environment). Any such specific assistance must be documented by the assessor.*	**Identify** the documentation and evidence examined in support of this test requirement, including the documentation and evidence examined in 1.1.a.		
	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.		
	Describe any discrepancies found between the information obtained through the documentation and evidence reviews and the information obtained through software testing.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
1.1.e The assessor shall examine vendor evidence and test the software to identify the transaction types and/or card data elements that are supported by the software. The assessor shall confirm that the data for all of these is supported by the vendor evidence.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe any discrepancies that were found between the information obtained through the documentation and evidence reviews and the information obtained through the software testing.		
1.1.f The assessor shall examine vendor evidence and test the software to identify the cryptographic implementations that are supported by the software, including (but not limited to) cryptography used for storage, transport, and authentication. The assessor shall confirm that the cryptographic data for all of these implementations is supported by the vendor evidence, and that the evidence describes whether these are implemented by the software itself, through third-party software, or as functions of the execution environment.	**Identify** the documentation evidence examined in support of this test requirement.		
	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.		
	Describe any discrepancies found between the information obtained through the documentation and evidence reviews and the information obtained through software testing.		
1.1.g The assessor shall examine vendor evidence and test the software to identify any accounts or authentication credentials supported by the software, including both default and user created accounts. The assessor shall confirm that these accounts and credentials are supported by the vendor evidence.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe any discrepancies found between the information obtained through the documentation and evidence reviews and the information obtained through software testing.		
1.1.h The assessor shall examine vendor evidence and test the software to identify any configuration options provided by the software that can impact sensitive data, including through separate files or scripts, or internal functions, menus and options provided by the software. The assessor shall confirm that these are supported by the vendor evidence.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe each of the configuration options that can impact the security of sensitive data.		
	Describe the criteria the assessor used to determine whether configuration options provided by the software have the potential to impact the security of sensitive data.		
	Describe any discrepancies found between the information obtained through the documentation and evidence reviews and the information obtained through software testing.		
1.1.i When cryptography is used to protect any sensitive data, the assessor shall examine vendor evidence to confirm that these cryptographic methods and materials are identified.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe any additional software tests performed in support of this test requirement, including the tool(s) or method(s) used and the scope of each test.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether cryptography is used by the software for protecting sensitive data.				
	Indicate whether the software uses cryptography to protect any sensitive data (yes/no).				
	If "yes," **identify** the documentation and evidence examined that identifies and describes all cryptographic methods and materials used to protect sensitive data.				
1.2 All sensitive functions and sensitive resources provided or used by the software are identified.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
1.2.a The assessor shall examine vendor evidence to confirm that it 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe any additional software tests performed in support of this test requirement, including the tool(s) or method(s) used and the scope of each test.				
	Describe what the assessor observed in the documentation, evidence and software test results that confirms that all software functions that are designed to store, process, and transmit sensitive data are documented.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
1.2.b For each of the sensitive functions and sensitive resources listed, the assessor shall examine vendor evidence to confirm that vendor evidence clearly describes how and where the sensitive data associated with these functions and resources is stored. This includes 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 information provided in Test Requirement 1.1.a.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe any discrepancies found between the sensitive data identified through the documentation and evidence reviews in 1.1.a and the sensitive data identified through the documentation and evidence reviews in 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 third-party software or system evidence and test the software to confirm that the vendor software is correctly following the guidance for this third-party software. ***Note:*** *For example, by reviewing the security policy of a PTS, FIPS 140-2, or FIPS 140-3 approved cryptographic system.*	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether any sensitive functions or sensitive resources are provided by third-party software or systems.		
	Indicate whether any sensitive functions or sensitive resources are provided by third-party software or systems (yes/no). *If "no," skip to 1.2.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that third-party software and resources have been implemented in the software in accordance with the third-party vendor's implementation guidance.		
1.2.d The assessor shall examine vendor evidence and test the software to confirm that the sensitive functions and sensitive resources provided or used by the software are supported by the vendor evidence.	**Describe** any documentation and evidence examined in support of this test requirement, including the documentation and evidence examined in 1.2.a.		
	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.		
	Describe any discrepancies found between the information obtained through the documentation and evidence reviews and the information obtained through software testing.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
1.3 Critical assets are classified.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
1.3 The assessor shall examine vendor evidence to confirm that: • The vendor defines classification criteria for identifying critical assets. • Vendor classification criteria identifies the confidentiality, integrity, and resiliency requirements for each critical asset. • An inventory of all critical assets with appropriate classifications is defined.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence examined that confirms the software vendor has identified the confidentiality, integrity, and resiliency requirements for each critical asset.				
	Describe how the software vendor's inventory of all critical assets is maintained (e.g., the format, location, etc.).				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 2: Secure Defaults Default privileges, features, and functionality are restricted to only those necessary to provide a secure default configuration.					
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** ☐	**N/A** ☐	**Not in Place** ☐
2.1.a The assessor shall examine vendor 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 functions, 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 functionality of the software (such as scanning for listening services where applicable). ***Note:*** *This includes functions which are auto-enabled as required during operation of the software.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe each of the tests performed in support of this test requirement, including tool(s) or method(s) used and the scope of each test.				
	Describe any discrepancies found between the information obtained through the documentation and evidence reviews and the information obtained through the software testing.				
2.1.b The assessor shall test the software to determine whether any of the functions identified in Test Requirement 2.1.a rely on external resources for authentication. If such resources are relied upon, the assessor shall examine vendor evidence to identify what methods are required to ensure proper authentication remains in place and shall confirm that these methods are included in the assessment of all other requirements of this standard.	**Identify** any documentation and evidence examined in support of this test requirement, including the documentation and evidence examined in 2.1.a.				
	Describe each of the software tests performed in support of this test requirement, including tool(s) or method(s) used and the scope of each test.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software relies on external resources for authentication.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Indicate whether the software relies upon such external resources for authentication (yes/no).		
	If "yes," **describe** each of the methods implemented by the software to ensure proper authentication remains in place for the APIs and other interfaces provided or exposed by the software.		
2.1.c The assessor shall test the software to determine whether any of the functions identified in Test Requirement 2.1.a rely on external resources for the protection of sensitive data during transmission. If such resources are relied upon, the assessor shall examine vendor evidence to identify what methods are required to ensure proper protection remains in place and shall confirm that these methods are included in the assessment of all other requirements of this standard.	**Identify** any documentation and evidence examined in support of this test requirement, including the documentation and evidence examined in 2.1.a.		
	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.		
	Describe what the assessor observed in the documentation, evidence and software test results that confirms determines whether any of the APIs or other interfaces identified in 2.1.a rely on external resources for the protection of sensitive data during transmission.		
	Indicate whether any of the APIs or other interfaces identified in 2.1.a rely on external resources for the protection of sensitive data during transmission (yes/no).		
	If "yes," **describe** each of the methods implemented to ensure proper protection of sensitive data remains in place and why the methods are appropriate for their intended purpose.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
2.1.d The assessor shall test the software to identify whether any of the functions identified in Test Requirement 2.1.a expose methods or services which 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.	**Identify** any documentation and evidence examined in support of this test requirement, including the documentation and evidence examined in 2.1.a.		
	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.		
	Identify the public vulnerability repositories that were searched (manually or electronically) in conjunction with the software testing in this test requirement.		
2.1.e Where vulnerabilities in exposed functions exist, the assessor shall examine vendor evidence and test the software to confirm the following: • The mitigations implemented by the software vendor to minimize exploit of these weakness have been identified. • The risks posed by the use of known vulnerable protocols, functions, or ports is documented. • Clear and sufficient guidance on how to correctly implement sufficient security to meet the security and control objectives of this standard is made available to stakeholders per Control Objective 12.1. ***Note:*** *The assessor should reference the vendor threat information defined in Control Objective 4.1 for this item.*	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether any vulnerabilities exist in exposed software functions, APIs, or other interfaces.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Indicate whether any of the functions, APIs, or other interfaces identified in 2.1.a expose methods or services (including protocols, functions, or ports), which have publicly disclosed vulnerabilities (yes/no). *If "no," skip to 2.1.f.* *If yes," complete the remaining reporting instructions for this test requirement.*		
	Describe each of the mitigations implemented in the software to mitigate the risks posed by the vulnerabilities in the exposed methods or services, and why each mitigation is appropriate for its intended purpose.		
	Describe the software vendor's justification for the software's use of known vulnerable functions, protocols, and ports, and how the assessor concluded the vendor's justification(s) are reasonable, given the risks involved.		
2.1.f The assessor shall examine vendor evidence and test the software to confirm available functionality matches what is described in vendor documentation. Testing shall include methods to reveal any exposed functionality of the software (such as scanning for listening services where applicable).	***Note:*** *This test requirement is redundant with test requirement 2.1.a. Reporting instructions are intentionally left blank. No further instruction needed.*		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
2.1.g The assessor shall examine vendor evidence for any third-party modules used by the software and ensure that any functionality exposed by each module is disabled, unable to be accessed through mitigation methods implemented by the software, or formally documented and justified by the vendor. Where access to third-party functions is prevented through implemented mitigations, the assessor shall test the software to confirm that they do not rely on a lack of knowledge of the functions as their security mitigation method—e.g., by simply not documenting an otherwise accessible API interface—and to verify the mitigations in place are effective at preventing the insecure use of such third-party functions.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all software functions exposed by third-party modules are either disabled or unable to be accessed by default.		
	Indicate whether any third-party modules or functions are exposed (through APIs or other interfaces) by default (yes/no). *If "no," skip to 2.2.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe each of the third-party modules or functions that are exposed by default and the software vendor's justification for doing so. For each instance where third-party modules or functions are exposed by default, also **describe** why the assessor considers the vendor's justification for each exception reasonable.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms mitigations are implemented to prevent the insecure use of exposed third-party modules or functions, and that such mitigations are appropriate for their given purpose.				
2.2 All software security controls, features, and functions are enabled upon software installation, initialization, or first use.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
2.2.a The assessor shall examine vendor evidence and test the software to identify all software security controls, features and functions, and to confirm that any such controls, features and functions relied upon by the software for the protection of critical assets are enabled upon installation, initialization, or first use of the software.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
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 no sensitive data can be processed until this initialization process has been completed.	**Indicate** whether any of the software security controls, features, and functions identified in 2.2.a are enabled only upon initialization or first use, rather than upon installation (yes/no). *If "no," skip to 2.2.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*				
	Describe any circumstances that exist that prevent security controls, features, and functions from being enabled upon installation (for example, the software is only available as a service).				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	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.		
2.2.c Where user input or interaction is required to enable any software security controls, features, or functions (such as the installation of certificates) the assessor shall examine vendor evidence to confirm that there is clear and sufficient guidance on the process provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Indicate** whether any of the software security controls, features, or functions identified in 2.2.a require user input or interaction prior to being enabled (yes/no). *If "no," skip to 2.2.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence examined in support of this test requirement.		
	Identify the documentation and evidence examined that contains the software vendor's implementation guidance for properly enabling each of the security controls, features, and functions that require user input or interaction prior to being enabled.		
2.2.d The assessor shall examine vendor evidence and test the software to confirm that following the software vendor's implementation guidance required in Control Objective 12.1 results in all security-relevant software security controls, features, and functions being enabled prior to the software enabling processing of sensitive data.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirm all security-relevant features, controls, and functions are enabled and active prior to the software enabling sensitive data processing.				
2.3 Default authentication credentials or keys for built-in accounts are not used after installation, initialization, or first use.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
2.3.a The assessor shall examine vendor evidence to identify all 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.*	**Identify** the documentation and evidence examined in support of this test requirement.				
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 vendor evidence. ***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 SBoxes 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.*	**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.				
	Describe any discrepancies found between the information obtained through the documentation and evidence reviews in 2.3.a and the information obtained through the software testing performed in this test requirement.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Indicate whether any authentication methods require user input or interaction to disable or change authentication credentials or keys for built-in accounts (yes/no). *If "no," skip to 2.3.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence examined that contains the software vendor's implementation guidance for disabling or changing all authentication credentials or keys for built-in accounts, where user input or interaction is required.		
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.*	**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.		
	Describe what the assessor observed in the software testing results that confirms that default authentication credentials or keys for built-in accounts are not used by the software after software installation, initialization, or first use.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
2.3.e The assessor shall test the software to confirm that default authentication credentials or keys for built-in accounts are not used to protect the storage and transmission of sensitive data. ***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.*	**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.				
	Describe what the assessor observed in the software testing results that confirms that default authentication credentials or keys for built-in accounts are not used to protect the storage and transmission of sensitive data after software installation, initialization, or first use.				
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** ☐	**N/A** ☐	**Not in Place** ☐
2.4.a The assessor shall examine vendor evidence to identify all privileges and resources required by the software and to confirm the evidence describes and reasonably justifies all privileges and resources required, including explicit permissions for access to resources, such as cameras, contacts, etc.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that indicates that the vendor's justifications for the privileges and resources required by the software are reasonable.				
2.4.b Where limiting access is not possible—e.g., due to the architecture of the solution or the execution environment in which the software is executed—the assessor shall examine vendor evidence to identify all mechanisms implemented by the software to prevent unauthorized access, exposure, or modification of critical assets, and to confirm there is clear and sufficient guidance on properly implementing the mechanisms provided in the software vendor's implementation guidance made available to stakeholders	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms whether the software requires elevated privileges to access any resources required by the software.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Indicate whether the software requires elevated privileges to access any resources required by the software (yes/no). *If "no," skip to 2.4.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe the mechanisms implemented by the software to prevent unauthorized access, exposure, or modification of critical assets.		
	Identify the documentation and evidence examined that contains the software vendor's implementation guidance on properly configuring such mechanisms.		
2.4.c The assessor shall test the software to confirm that access permissions and privileges are assigned according to the vendor evidence. 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.*	**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.		
	Describe any discrepancies between the information obtained through the documentation and evidence reviews in 2.4.a and the information obtained through the software testing in this test requirement.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
2.4.d Where the software execution environment provides legacy features for use by older versions of the software, the assessor shall examine vendor evidence and test the software to confirm that these are not utilized, and only recent and secured functionality is implemented. For example, software should "target" the latest versions of APIs provided by the environment they run on, where available.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe *each of the tests performed in support of this test requirement, including the tool(s) or method(s) used and the scope of each test.*				
	Describe what the assessor observed in documentation, evidence and software test results that confirms that the software does not use legacy features of the intended execution environment, and that only recent and secured functions are implemented.				
2.5 Default privileges for built-in accounts are limited to those necessary for their intended purpose or function.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
2.5.a The assessor shall examine the vendor evidence to identify all default accounts provided by the software and to confirm vendor evidence includes reasonable justification for the privileges assigned to these accounts.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that indicates that the software vendor's justifications for the privileges assigned to each of the default accounts are reasonable.				
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 vendor evidence.	**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.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe any discrepancies between the information obtained through the documentation and evidence reviews in 2.5.a and the information obtained through the software testing in this test requirement.		
2.5.c The assessor shall examine vendor evidence and test the software to confirm that exposed functionalities (i.e., APIs) are protected from use by unauthorized users to modify account privileges and elevate user access rights.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in documentation, evidence, and software test results that confirms that all exposed software functions (APIs and other interfaces) are protected from unauthorized use and modification.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 3: Sensitive Data Retention Retention of sensitive data is minimized.					
3.1 The software only retains the sensitive data absolutely necessary for the software to provide its intended functionality.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
3.1.a The assessor shall examine vendor evidence to identify what sensitive data 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 vendor evidence includes reasonable justification for retaining the sensitive data. ***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.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that indicates that the vendor's justifications for retaining each item of persistent sensitive data are reasonable.				
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 vendor evidence. ***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.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe any discrepancies found between the functions and services identified through the documentation and evidence reviews and the functions and services identified through the software testing.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
3.1.c The assessor shall test the software to confirm that sensitive data stored solely for the purposes of debugging, error finding, or testing of systems is protected during storage in accordance with Control Objective 6. Any such functionality that allows for storage of sensitive data must be explicitly enabled through an interface that requires interaction and authorization by the user and retained 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether the software facilitates the storage and/or retention of persistent sensitive data for debugging, error finding, or testing purposes (yes/no). *If "no," skip to 3.1.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that all persistent sensitive data stored or retained for debugging, error finding, or testing purposes are protected in accordance with Control Objective 6.		
	Describe the software configuration options, mechanisms, etc., that must be enabled explicitly and authorized by the user before any storage and/or retention of persistent sensitive data is permitted by the software.		
	Describe the specific features and functions implemented by the software to ensure that all persistent sensitive data retained for debugging, error finding, or testing are securely deleted upon closure of the software in accordance with Control Objective 3.4.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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.	**Identify** the documentation and evidence examined that identifies and describes all instances in the software in which user input or interaction is required to configure the retention period of persistent sensitive data.		
	Indicate whether the software requires user input or interaction to configure the retention period for any persistent sensitive data stored or retained by the software (yes/no). *If "no," skip to 3.2.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence examined that contains the software vendor's implementation guidance for configuring the retention periods for persistent sensitive data stored or retained by the software.		
	Describe what the assessor observed in the software vendor's guidance that indicates clear and sufficient instruction is provided to stakeholders on configuring the retention periods of persistent sensitive data and the secure deletion procedures of the software.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
3.2 Transient sensitive data is retained only for the duration necessary to fulfill a legitimate business purpose.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
3.2.a The assessor shall examine vendor evidence to identify all sensitive data that is retained by the software for transient use, what triggers the secure deletion of this data, and confirm reasonable justification exists for retaining the data. This includes data that is stored only in memory during the operation of the software. ***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets, including transient sensitive data.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence examined that indicates that the software vendor's justifications for retaining each item of sensitive data for transient use are reasonable.				
3.2.b The assessor shall test the software to confirm that all available functions or services that retain transient sensitive data are supported by vendor evidence and do not use immutable objects. ***Note:*** *The assessor should refer to Control Objective 1 to identify all sensitive functions and services.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the software test results that confirms the software does not use immutable objects to store transient sensitive data.				
	Describe any discrepancies found between the functions and services for retaining transient sensitive data identified through the documentation and evidence reviews in 3.2.a and the functions and services for retaining transient sensitive data identified through the software testing in this test requirement.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
3.2.c The assessor shall test the software to confirm that transient sensitive data stored solely for the purposes of debugging, error finding, or testing of systems is protected in accordance with Control Objective 6. Any such functionality that allows for the storage of transient sensitive data must be explicitly enabled through an interface that requires interaction and authorization by the user. 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 transient sensitive data is securely deleted in accordance with Control Objective 3.4.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	I**ndicate** whether the software facilitates the storage or retention of transient sensitive data for debugging, error finding, or testing (yes/no). *If "no," skip to 3.2.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicate that all transient sensitive data stored or retained for debugging, error finding, or testing purposes are protected in accordance with Control Objective 6.		
	Describe the software configuration options, mechanisms, etc., that must be enabled explicitly and authorized by the user before any storage and/or retention of transient sensitive data for debugging, error finding, or testing is permitted.		
	Describe the specific features and functions implemented by the software to ensure that all transient sensitive data retained for debugging, error finding, or testing is securely deleted upon closure of the software in accordance with Control Objective 3.4.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms determines whether the software enables users to configure retention periods for transient sensitive data.		
	Indicate whether the software enables users to configure the retention periods for transient sensitive data (yes/no). *If "no," skip to 3.3.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence examined that contains the software vendor's implementation guidance for configuring the retention periods for transient sensitive data stored or retained by the software.		
	Describe what the assessor observed in the software vendor's implementation guidance that indicates clear and sufficient instruction is provided to stakeholders on configuring the retention periods for transient sensitive data and configuring the secure deletion of such data when no longer needed.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
3.3 The software protects the confidentiality and integrity of sensitive data (both transient and persistent) during retention.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
3.3.a The assessor shall examine the vendor evidence to identify the protection methods implemented for all sensitive data during storage and transmission.	**Identify** the documentation and evidence examined in support of this test requirement.				
3.3.b The assessor shall test the software to confirm that no additional storage of sensitive data is included.	**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.				
	Describe what the assessor observed in the software testing results that confirms the software does not provide for any additional storage or retention of sensitive data beyond that which was identified in the testing for Control Objectives 3.1 and 3.2.				
3.3.c 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether any transient sensitive data is stored outside of temporary variables during retention.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Indicate whether any sensitive data (persistent or transient) are stored outside of temporary variables during retention (yes/no). *If "no," skip to 3.3.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the software structures and locations used to store each item of sensitive data (persistent or transient), where such data is stored outside of temporary variables during retention.		
	For each item of sensitive data (persistent or transient) that is stored outside of temporary variables during retention, **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that all instances of sensitive data stored outside of temporary variables during retention are protected using either strong cryptography or other methods that provide equivalent security.		
3.3.d Where protection methods use cryptography, the assessor shall examine vendor evidence and test the software to confirm that the cryptographic implementation complies with Control Objective 7 of this standard.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Indicate whether cryptography is used by the software to protect any sensitive data stored or retained by the software (yes/no). *If "no," skip to 3.3.e.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the cryptographic methods used to protect sensitive data stored or retained by the software.		
	For each of the cryptographic methods used, **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that each cryptographic implementation complies with Control Objective 7.		
3.3.e Where sensitive data is protected using methods other than strong cryptography, the assessor shall examine vendor evidence and test the software to confirm that the protections are present in all environments where the software is designed to be executed, are correctly implemented, and are covered by the vendor evidence.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether protection methods other than strong cryptography are used to protect any sensitive data during storage or retention (yes/no). *If "no," skip to 3.3.f.* *If "yes," complete the remaining reporting instructions for this test requirement.*		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that protections are present in each of the execution environments evaluated and are implemented correctly.		
	Describe any discrepancies found between the protection methods identified through the documentation and evidence reviews and the protection methods identified through the software testing.		
3.3.f Where users are required to configure protection methods, 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether the software requires user input or interaction to configure the protection methods identified in 3.3.a, 3.3.d and 3.3.e (yes/no). *If "no," skip to 3.4.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence examined that contains the software vendor's implementation guidance for instructing users where and how to configure all protection mechanisms that require user input or interaction.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the software vendor's implementation guidance that indicates that the instructions for configuring all such protection methods are appropriate and sufficient to result in the secure configuration of the applicable protection methods.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
3.4 The software securely deletes sensitive data when it is no longer required.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
3.4.a The assessor shall examine vendor evidence to identify all secure deletion methods implemented by the software for all non-transient sensitive data.	**Identify** the documentation and evidence examined that identifies and describes all methods implemented by the software to securely delete non-transient sensitive data when no longer required.				
3.4.b The assessor shall examine vendor 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 unrecoverable after deletion. Methods may include (but are not necessarily limited to) overwriting the data, deletion of cryptographic keys (of sufficient strength) which have been used to encrypt the data, or platform specific functions which 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe any additional software tests performed to support of this test requirement, including the tool(s) or method(s) used and the scope of each test.				
	Indicate whether there are any platform or implementation level issues that may complicate the secure deletion of non-transient sensitive data (yes/no). *If "no," skip to 3.4.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*				
	Identify all platform and implementation issues that may complicate the erasure of transient sensitive data.				
	Identify the methods implemented to ensure non-transient sensitive data is rendered unrecoverable.				
	Describe how the methods to render transient sensitive data unrecoverable accommodate for platform-specific issues, such as flash wear-levelling algorithms or SSD over-provisioning.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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 (e.g., by examining file systems at the allocation level, and translating data formats to identify sensitive data elements), as well as covering 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.*	**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.		
	Describe what the assessor observed in the software testing results that confirms the methods implemented by the software to render non-transient sensitive data unrecoverable are implemented correctly.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
3.5.a The assessor shall examine vendor evidence to identify all secure deletion methods for all transient sensitive data and to confirm that these methods ensure that the data is unrecoverable after deletion. ***Note:*** *This includes data which may be stored only temporarily in program memory / variables during operation of the software.*	**Identify** the documentation and evidence examined in support of this test requirement.				
3.5.b The assessor shall examine vendor 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 what methods have been implemented to minimize the risk posed by these complications.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Indicate whether there are any platform or implementation level issues that may complicate the erasure of transient sensitive data (yes/no). *If "no," skip to 3.5.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*				
	Identify all platform and implementation issues that complicate the erasure of transient sensitive data.				
	Identify each of the methods implemented to minimize the risk posed by these complications.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
3.5.c The assessor shall test the software, including usage of forensic tools, to identify any sensitive data residue in the execution environment to confirm that the methods attested by the software vendor are correctly implemented and applied to all transient sensitive data. This analysis should accommodate for the data structures and methods used to store the sensitive data—e.g., by examining file systems at the allocation level, and translating data formats to identify sensitive data elements—as well as 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.*	**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.		
	Describe what the assessor observed in in the software testing results that confirms that the methods implemented by the software to render transient sensitive data unrecoverable are implemented correctly and applied to all transient sensitive data.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
3.6 The software does not disclose sensitive data through unintended channels.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
3.6.a The assessor shall examine vendor 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, etc. • 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, near-field communication (NFC) interfaces, etc.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms the software vendor's analysis accounts for the attack vectors described in this test requirement.				
	Identify any additional sensitive data disclosure attack vectors covered in the vendor's analysis.				
	Identify the date(s) when the software vendor's analysis was last updated.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
3.6.b The assessor shall examine vendor evidence, including the results of the analysis described in Test Requirement 3.6.a, and test the software to confirm the software vendor implements mitigations to protect against unintended disclosure of sensitive data. Mitigations 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).	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicate that the mechanisms that protect against the unintended disclosure of sensitive data are implemented correctly.		
3.6.c The assessor shall examine vendor evidence to confirm that clear and sufficient guidance on the proper configuration and use of such mitigations is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms the software vendor's guidance is appropriate and sufficient to result in the secure configuration and use of all such mitigations.		
3.6.d The assessor shall test the software using forensic tools to identify any sensitive data residue in the execution environment, and to confirm that all mitigation controls are correctly implemented and the software does not expose or otherwise reveal sensitive data.	**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.		
	Describe what the assessor observed in the software testing results that confirms that all mitigation controls that protect against the unintended disclosure of sensitive data are implemented correctly.		

Software Protection Mechanisms

Software security controls are implemented to protect the integrity and confidentiality of critical assets.

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 4: Critical Asset Protection Critical assets are protected from attack scenarios.					
4.1 Attack scenarios applicable to the software are identified.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
4.1.a The assessor shall examine vendor evidence to confirm that the software vendor has identified, documented, and prepared mitigations for relevant attack scenarios for the software.	**Identify** the documentation and evidence examined that identifies and describes all software attack scenarios and the protection mechanisms implemented to mitigate those attacks.				
4.1.b The assessor shall examine vendor evidence to determine whether any specific industry-standard methods or guidelines were used to identify relevant attack scenarios, such as the threat model guidelines. Where such industry standards are not used, the assessor shall confirm that the methodology used provides an equivalent coverage of the attack scenarios and methods for the software.	**Identify** the documentation and evidence examined that identifies and describes the vendor's method(s) for determining software attack scenarios.				
	Indicate whether industry-standard methods are the basis for the software vendor's method(s) (yes/no).				
	If "yes," **identify** the industry-standard methods or guidelines used.				
	If "no," **describe** how the software vendor's method(s) provides coverage of the software attack scenarios that is equivalent to industry-standard methods.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
4.1.c The assessor shall examine the vendor 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 by and all sensitive resources used by the system are documented. • All entry and egress methods for sensitive data by the software, as well as the authentication and trust model applied to each of these entry/egress points, are defined. • All data flows, network segments, and authentication/privilege boundaries are defined. • All static IPs, domains, URLs, or ports required by the software for operation are documented. *(continued on next page)*	**Identify** the documentation and evidence examined in support of this test requirement.		
	Identify the individual who is assigned formal ownership for the software under evaluation.		
	Summarize the software vendor's method(s) for defining and measuring the probability and impact of potential exploits against the assessed software.		
	Describe what the assessor observed in the documentation and evidence that indicates that all sensitive data entry and egress points and the authentication and trust model(s) applied to these points are covered in the vendor's attack analysis.		
	Describe what the assessor observed in the documentation and evidence that indicates that all software data flows, network segments, and authentication/privilege boundaries are covered in the software vendor's attack analysis.		
	Describe what the assessor observed in the documentation and evidence that indicates that all static IPs, domains, URLs, or ports required by the software for operation were covered in the vendor's attack analysis.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
• Considerations for cryptography elements like cipher modes, protecting against timing attacks, padded oracles, brute force, "rainbow table" attacks, dictionary attacks against the input domain, etc. are documented. • Execution environment implementation specifics or assumptions such as network configurations, operating system security configurations, etc. are documented. • Consideration for the installed environment of the software, including any considerations for the size of the install base are documented. All attack surfaces that must be mitigated—such as implementing insecure user prompts or separating open protocol stacks; storage of sensitive data post authorization or storage of sensitive data using insecure methods, etc.—are documented.	**Describe** what the assessor observed in the documentation and evidence that indicates that cryptography and cryptographic elements, such as cipher modes, were considered in the vendor's attack analysis.		
	Describe what the assessor observed in the documentation and evidence that indicates that the software execution environment was considered in the vendor's attack analysis.		
	Describe what the assessor observed in the documentation and evidence that indicates that the software vendor's attack analysis covers the use of insecure methods.		
4.1.d The assessor shall examine vendor evidence to confirm that the threat model created is reasonable to address the potential risks posed by the install and use of the software in a production environment—i.e., not in a test environment—given the assessor's understanding through evaluation of the payment software to this standard.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence examined that indicates that the risks that are unique to a production deployment of the assessed software are considered in the vendor's attack analysis.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
4.2 Software security controls are implemented to mitigate software attacks.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
4.2.a The assessor shall examine vendor evidence to confirm that for each of the threats identified in Control Objective 4.1, one or more mitigation methods are clearly defined, or reasonable justification for the lack of mitigations is provided.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Indicate whether any of the threats identified in Control Objective 4.1 were not mitigated (yes/no).				
	If "yes," **describe** what the assessor observed in the documentation and evidence that indicates that the vendor's justification(s) for any lack of mitigation is reasonable.				
4.2.b The assessor shall examine vendor evidence and test the software to confirm that the implemented mitigation methods are reasonable for the threat they address.	**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.				
	Describe what the assessor observed in the documentation, evidence and software test results that indicates that the implemented mitigation methods are appropriate for the threats they are intended to address.				
4.2.c Where any mitigations rely on settings within the software, the assessor shall test the software to confirm that such settings are applied by default, before first processing any sensitive data, upon installation, initialization, or first use of the software. *(continued on next page)*	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
Where user input or interaction can disable, remove, or bypass any such mitigations, the assessor shall test the software to confirm that such action requires authorization and strong authentication, and examine vendor evidence to confirm that clear and sufficient guidance on the risk of this action and that installation in this manner will invalidate any security validation that has been performed is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Describe** what the assessor observed in the documentation, evidence, and software test results that confirms whether any software mitigations or protection mechanisms rely on configurable settings within the software.		
	Indicate whether any of the mitigations identified in 4.2.a rely on software configuration settings or values (yes/no). *If "no," skip to 4.2.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicate that all settings and values required to configure such mitigations are applied by default.		
	Indicate whether any such settings and mitigations can be disabled, removed, or bypassed by user input or interactions (yes/no). *If "no," skip to 4.2.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that settings or values required to configure threat mitigations cannot be disabled, removed, or bypassed without requiring strong user authentication and authorization.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Identify the documentation and evidence examined that contains the software vendor's guidance on configuring threat mitigations and the risks and impacts of disabling, removing, or bypassing such mitigations.		
4.2.d When any mitigations rely on features of the execution environment, the assessor shall examine vendor evidence to confirm that guidance is provided to the software users to enable such settings as part of the install process. Where the execution environment provides APIs to query the status of mitigation controls, the assessor shall test the software to confirm that software checks that these mitigations are in place and active prior to being launched, and periodically throughout execution.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether software protection mechanisms rely on features of the execution environment.		
	Indicate whether any protection mechanisms rely on features of the execution environment (yes/no). *If "no," skip to 5.1.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence that contains the software vendor's guidance on enabling, configuring, and using protection methods provided by the execution environment.		
	Indicate whether the intended execution environment provides any APIs to query the status of mitigation controls (yes/no).		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	If 'yes," **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that the software performs checks to verify mitigation controls are in place and active upon start up and periodically throughout software execution.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 5: Authentication and Access Control The software implements strong authentication and access control to help protect the confidentiality and integrity of critical assets.					
5.1 Access to critical assets is authenticated.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
5.1.a The assessor shall examine vendor evidence to confirm that the vendor has identified authentication requirements (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.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that authentication requirements are defined for all roles based on critical-asset classification, type of access, and level of privilege.				
5.1.b The assessor shall examine vendor evidence and test the software to confirm that all access to critical assets is authenticated and authentication mechanisms are implemented correctly.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation, evidence, and software test results that indicate that each of the authentication mechanisms are implemented correctly.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
5.1.c Where the software recommends, suggests, relies on, or otherwise facilitates the use of additional mechanisms (such as third-party VPNs, remote desktop features, etc.) to facilitate secure non-console access to the system on which the software is executed or directly to the software itself, the assessor shall examine vendor evidence to confirm that clear and sufficient guidance on how to configure authentication mechanisms correctly is provided in the software vendor's implementation guidance documents made available to stakeholders per Control Objective 12.1.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether the software relies on or supports the use of additional mechanisms for secure non-console access to the software (yes/no). *If "no," skip to 5.1.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence that contains the software vendor's guidance on configuring additional authentication mechanisms for secure non-console access to the software.		
5.1.d The assessor shall examine vendor evidence to confirm that any sensitive data associated with credentials, including public keys, is identified as a critical asset.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that indicates that all data associated with authentication credentials is treated as a critical asset.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
5.2 Access to critical assets requires unique identification.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
5.2.a The assessor shall examine vendor evidence and test the software to confirm that all implemented authentication methods require unique identification.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the vendor observed in the documentation, evidence, and software test results that confirms that all implemented authentication methods require unique identification.				
5.2.b Where interfaces, such as APIs, allow for automated access to critical assets, the assessor shall examine vendor 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 included in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Indicate whether the software provides APIs or other interfaces to enable automated access to critical assets (yes/no). *If "no," skip to 5.2.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that access to the software's critical assets by different programs or systems requires unique identification and authentication.		
	Identify the documentation and evidence that contains the software vendor's guidance on configuring unique credentials for each program or system to which automated access to critical assets is provided via APIs or other interfaces.		
5.2.c Where identification is supplied across a non-console interface, the assessor shall test the software to confirm that authentication mechanisms are protected.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether identification is supplied across a non-console interface (yes/no).		
	If "yes," **describe** what the assessor observed in the documentation, evidence, and software test results that indicate that the authentication mechanisms that supply its identification parameters in this way are protected.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
5.2.d The assessor shall examine vendor evidence to confirm that software vendor's implementation 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.	**Identify** the documentation and evidence examined that contains the software vendor's guidance on the use of identification and authentication parameters.		
	Describe what the assessor observed in the software vendor's guidance that confirms that users are instructed not to share identification and authentication parameters between individuals or programs.		
5.2.e The assessor shall examine vendor evidence, including source code of the software, to confirm that there are no additional methods for accessing critical assets.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe how and the extent to which source code was examined to confirm that the software provides no other methods for accessing critical assets.		
	Describe what the assessor observed in the documentation, evidence, and source code that indicates that the software provides no additional methods, other than those identified in 5.2.a.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
5.3.a The assessor shall examine vendor evidence to confirm that all implemented authentication methods were evaluated to identify the details of known vulnerabilities or attack methods on the authentication method, and how the implementation mitigates against such attacks. The evidence must also illustrate that 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the implementation of each authentication method was evaluated to identify known vulnerabilities, attack methods, vectors, or patterns that might enable an attacker to compromise or, otherwise, circumvent the authentication method.				
	Describe what the assessor observed in the documentation and evidence that indicates that the protection mechanisms implemented to mitigate the probability and impact of potential attacks on the software's authentication methods are appropriate for their intended purpose and that any residual risk has been reasonably justified.				
5.3.b The assessor shall examine vendor evidence to confirm that implemented authentication methods are robust and that robustness of the authentication methods was evaluated using industry-accepted methods.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe the methods used by the software vendor to evaluate the robustness of the implemented authentication methods and how they are consistent with industry-accepted methods.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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).*	**Describe** what the assessor observed in the documentation and evidence that indicates that the implemented authentication methods are reasonably sufficient to protect them from being forged, spoofed, leaked, guessed, or circumvented.		
5.3.c The assessor shall test the software to confirm the authentication methods are implemented correctly and do not expose vulnerabilities.	**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.		
	Describe what the assessor observed in the software test results that provides reasonable assurance that the authentication mechanisms are implemented correctly and do not expose vulnerabilities.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
5.4 By default, all access to critical assets is restricted to only those accounts and services that require such access.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
5.4.a The assessor shall examine vendor evidence to confirm that the vendor has clearly identified and reasonably justified the required access for all critical assets.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that indicates that the access requirements and justification(s) for each critical asset are reasonable for the software's intended function.				
5.4.b The assessor shall examine vendor evidence and test the software to identify what access is provided to critical assets and confirm that such access correlates with the vendor evidence. The test to confirm access is restricted should include attempts to access critical assets through user accounts, roles, or services which should not have the required privileges.	**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.				
	Describe any discrepancies found between the access provided to critical assets identified through the documentation and evidence reviews and the access to critical assets identified through the software testing performed in support of this test requirement.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 6: Sensitive Data Protection Sensitive data is protected at rest and in transit.					
6.1 Sensitive data is secured anywhere it is stored.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
6.1.a The assessor shall examine vendor evidence and test the software to identify all locations where sensitive data is stored to confirm protection requirements for all sensitive data are defined, including requirements for rendering sensitive data with confidentiality considerations unreadable anywhere it is stored persistently.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation and evidence that indicates that protection requirements for all sensitive data stored by the software are defined.				
6.1.b The assessor shall examine vendor evidence and test the software to confirm that security methods implemented to protect all sensitive data during storage appropriately address all defined protection requirements and identified attack scenarios. ***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets and Control Objective 4 to identify all attack scenarios applicable to the software.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that security methods implemented to protect sensitive data during persistent storage properly address all defined protection requirements and identified attack scenarios.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
6.1.c Where cryptography is used for securing sensitive data, the assessor shall examine vendor evidence and test the software to confirm that any method implementing cryptography for securing sensitive data complies with Control Objective 7.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Based on the documentation, evidence, and the results of the software testing performed in support of this test requirement, **indicate** whether cryptography is used by the software for securing sensitive data during persistent storage (yes/no). *If "no," skip to 6.1.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and the software test results that indicates that in all instances where cryptography is used for securing sensitive data during persistent storage, the cryptography implementation complies with Control Objective 7.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
6.1.d Where index tokens are used for securing sensitive data, the assessor shall examine vendor 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 being referenced (without access to the vendor software to perform correlation as part of a formally defined and assessed feature of that software – such as "de-tokenization").	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether the software uses index tokens for securing sensitive data during persistent storage (yes/no). *If "no," skip to 6.1.e.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that index tokens are generated in a way that ensures there is no correlation between the value and the sensitive data being referenced.		
6.1.e Where protection methods rely on security properties of the execution environment, the assessor shall examine vendor evidence and test the software to confirm that these security properties are valid for all platforms which the software targets, and that they provide sufficient protection to the sensitive data.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether software protection mechanisms rely on execution environment security properties to safeguard sensitive data.		
	Indicate whether any protection mechanisms implemented by the software to safeguard sensitive data rely on execution environment security properties (yes/no). *If "no," skip to 6.1.f.* If "yes," complete the remaining reporting instructions for this test requirement.		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that the security properties, upon which the protection mechanisms rely, exist for all platforms included in the software evaluation.		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that the protection mechanisms that rely on execution environment security properties are appropriate for the type of sensitive data they are to protect.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
6.1.f Where protection methods rely on security properties of third-party software, the assessor shall examine vendor evidence and test the software to confirm that this software provides security that is sufficient to meet the requirements of this standard. The assessor shall perform a review of current publicly available literature and vulnerability disclosures to confirm that there are no unmitigated vulnerabilities or issues with the security properties relied upon with that software.	**Identify** the documentation and evidence examined for this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether software protection mechanisms rely on third-party software security properties to safeguard sensitive data.		
	Indicate whether protection mechanisms implemented by the software to safeguard sensitive data rely on third-party software security properties (yes/no). *If "no," skip to 6.2.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that the protection mechanisms that rely on third-party software security properties are appropriate for the type of sensitive data they are to protect.		
	Describe what the assessor observed in the documentation and evidence that confirms that there are no unmitigated vulnerabilities in the third-party software, whose security properties are relied upon by the software's protection methods.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
6.2 Sensitive data is secured during transmission.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
6.2.a The assessor shall examine vendor evidence and test the software to identify all locations within the software where sensitive data is transmitted and confirm protection requirements for the transmission of all sensitive data are defined.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation and evidence that confirms protection requirements are defined for all locations where the software transmits sensitive data.				
6.2.b The assessor shall examine vendor evidence and test the software to confirm that for each of the ingress and egress methods that allow for transmission of sensitive data with confidentiality considerations outside of the physical execution environment, sensitive data is always encrypted with strong cryptography prior to transmission or is transmitted over an encrypted channel 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.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all transmissions of sensitive data outside of the physical execution environment are encrypted prior to transmission using strong cryptography or are transmitted over an encrypted channel that uses strong cryptography.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
6.2.c Where third-party or execution-environment features are relied upon for the security of the transmitted data, the assessor shall examine vendor evidence to confirm that clear and sufficient guidance on how to configure such features are included in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe any additional software tests performed to support of this test requirement, including the tool(s) or method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software relies upon third-party or execution environment features for securing sensitive data during transmission.		
	Indicate whether the software relies upon any third-party or execution-environment features to ensure the security of transmitted sensitive data (yes/no). *If "no," skip to 6.2.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence that contains the software vendor's guidance on the configuration and use of all third-party or execution-environment features to protect transmitted sensitive data.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
6.2.d Where transport layer encryption is used to secure the transmission of sensitive data, the assessor shall test the software to confirm that all ingress and egress methods enforce a secure version of the protocol with end-point authentication prior to the transmission of that sensitive data.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether transport layer encryption is used to secure the transmission of sensitive data.		
	Indicate whether transport layer encryption is used (TLS) to secure the transmission of sensitive data (yes/no).		
	If "yes," **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that all ingress and egress methods used to transmit sensitive data enforce secure versions of the TLS protocol with end-point authentication.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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 test the software, including capturing software transmissions, to confirm the software enforces the use of strong cryptography at all times during transmission.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether software methods that encrypt sensitive data for transmission allow for different types of cryptography or different levels of security to be used.		
	Indicate whether the methods implemented by the software to encrypt sensitive data for transmission allow for the use of different types of cryptography or different levels of security (yes/no). *If "no," skip to 6.3.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all forms of cryptography used for encrypting sensitive data transmissions are strong cryptography.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms strong cryptography is enforced at all times by the software during transmission.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
6.3 Use of cryptography meets all applicable cryptography requirements within this standard.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
6.3.a The assessor shall examine vendor evidence and test the software to confirm that each use of cryptography—where cryptography is relied upon (in whole or in part) for the security of critical assets—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.*	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation, evidence, and software test results that indicate that all uses of cryptography for the purpose of securing critical assets complies with Control Objective 7.				
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 vendor evidence and test the software to confirm that the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1 provides clear and sufficient detail for correctly configuring these methods during the installation, initialization, or first use of the software.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software relies upon third-party software, platforms, or libraries for cryptographic services.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Indicate whether the software relies upon third-party software or aspects of the execution environment or platform for cryptographic services to protect sensitive data (yes/no).		
	If "yes," **identify** the documentation and evidence that contains the software vendor's guidance on the configuration and use of third-party or platform-provided cryptographic services to protect sensitive data.		
6.3.c Where asymmetric cryptography such as RSA or ECC is used for protecting the confidentiality of sensitive data, the assessor shall examine vendor evidence and test the software to confirm that private keys are not used for providing confidentiality protection to the data.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether asymmetric cryptography (such as RSA or ECC) is used for to protect the confidentiality of sensitive data (yes/no).		
	If "yes," **describe** what the assessor observed in the documentation, evidence, and software test results that confirms private keys are not used to provide confidentiality protection for sensitive data.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 7: Use of Cryptography Cryptography is used appropriately and correctly.					
7.1 Approved cryptographic algorithms and methods are used for securing critical assets. Approved cryptographic algorithms and methods are those recognized by industry-accepted standards bodies—for example: NIST, ANSI, ISO, and EMVCo. Cryptographic algorithms and parameters that are known to be vulnerable are not used.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
7.1.a The assessor shall examine the vendor evidence to confirm that, where cryptography is relied upon (in whole or in part) for the security of the critical assets: • Industry-accepted cryptographic algorithms and modes of operation are used in the software as the primary means for protecting critical assets; and • Use of any unapproved algorithms must be in conjunction with approved algorithms and implemented in a manner that does not reduce the equivalent cryptographic key strength provided by the approved algorithms.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Identify the industry-accepted cryptographic algorithms and modes of operation that are used in the software.				
	Indicate whether the software uses any unapproved cryptographic algorithms or modes of operation to protect critical assets (yes/no). *If "no," skip to 7.1.b.* *If "yes," complete the remaining reporting instructions for this test requirement.*				
	Identify each of the unapproved algorithms or modes of operation used to protect critical assets.				
	For each unapproved algorithm or mode of operation used to protect critical assets, **describe** how each is used with approved algorithms to ensure a cryptographic key strength is equivalent to that of the approved algorithms.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
7.1.b The assessor shall examine vendor evidence, including the vendor threat information, and test the software to confirm that: • Only documented cryptographic algorithms and modes are used in the software and are implemented correctly, and • Protections are incorporated to prevent common cryptographic attacks such as 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).	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that only documented cryptographic algorithms and modes of operation are used in the software.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that the cryptographic algorithms and modes of operation in use are implemented correctly (that is, fit-for-purpose).		
	Describe the mechanisms implemented to protect the cryptographic algorithms and modes of operation used by the software against common cryptographic attacks.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
7.1.c Where any algorithm or mode of operation requires a unique value per encryption operation or session, the assessor shall examine current publicly available literature or industry standards to identify security vulnerabilities in their implementation and test the software to confirm correct implementation. For example, this may include the use of a unique IV for a stream cipher mode of operation, a unique (and random) "k" value for a digital signature.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether any of the implemented cryptographic algorithms and supporting modes of operation require a unique value per encryption operation or session (yes/no). *If "no," skip to 7.1.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	For each of the cryptographic algorithms or modes of operation that require a unique value per encryption operation or session, **describe** how the implementation of those algorithms and modes of operation protect against common cryptographic attacks.		
7.1.d Where padding is used prior to/during encryption, the assessor shall examine vendor evidence and test the software to confirm that the encryption operation always incorporates an industry-accepted standard padding method.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Indicate whether the software uses padding prior to or during encryption operations (yes/no). *If "no," skip to 7.1.e.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that whenever an encryption operation uses padding, it always uses an industry-accepted standard padding method.		
	Identify each of the industry-accepted padding methods used by the software.		
7.1.e Where hash functions are used within the software, the assessor shall: • Examine publicly available literature and research to identify vulnerable algorithms that can be exploited, and • Test the software to confirm that only approved, collision-resistant hash algorithms and methods are used with a salt value of appropriate strength, generated using a secure random number generator. ***Note:*** *The assessor should refer to Control Objective 7.3 for more information on secure random number generators.*	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether the software uses any hash functions for the protection of sensitive data (yes/no). *If "no," skip to 7.2.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify each of the approved, collision-resistant hash algorithms and methods used by the software for the protection of sensitive data.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all hash algorithms that are used, leverage a salt value of approved strength that is generated using a secure random number generator.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
7.2 The software supports approved key-management processes and procedures. Approved key-management processes and procedures are those recognized by industry-standards bodies—for example: NIST, ANSI, and ISO.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
7.2.a The assessor shall examine vendor evidence and test the software to confirm that: • All cryptographic keys that are used for providing security to critical assets—including both confidentiality and authenticity—as well as for providing other security services to the software (such as authentication of end-point or software updates) have a unique purpose. For example, no key may be 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 (e.g., white-box cryptography). • All cryptographic keys have an equivalent bit strength of at least 128 bits in accordance with industry standards. *(continued on next page)*	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe each of the software tests performed in support of this test requirement, including the tool(s)j or method(s) used and the scope of each test.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all cryptographic keys that provide security to critical assets or other security services to the software have a unique purpose.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all keys have defined generation methods, and no secret or private cryptographic keys are relied upon for the security of critical assets that are shared between software instances, except when a common secret or private key is used to secure the storage of other cryptographic keys that are generated during the installation, initialization, or first use of the software.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
• All keys have a defined crypto-period aligned with industry standards, and methods are implemented to retire and/or update each key at the end of the defined crypto-period. • The integrity and confidentiality of all secret and private cryptographic keys managed by the software are protected when stored (e.g., 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.	**Describe** what the assessor observed in the documentation, evidence, and software test results that confirms that all cryptographic keys have an equivalent bit strength of at least 128 bits, in accordance with industry standards		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all keys have a defined crypto-period aligned with industry standards, and that methods are implemented to retire and/or update each key at the end of the defined crypto-period.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that the integrity and confidentiality of all secret and private cryptographic keys managed by the software are protected when stored.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all keys have a defined generation or injection process, and that the process ensures sufficient entropy for the key.		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that all key-generation functions implement one-way functions or other irreversible key-generation processes, and that no reversible key calculation modes are used to directly create new keys from an existing key.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
7.2.b Where cryptography is used to protect a key, the assessor shall examine vendor evidence and test the software to confirm that security is not provided to any key by a key of lesser strength (e.g., by encrypting a 256-bit AES key with a 128-bit AES key).	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software uses cryptography to protect cryptographic keys.		
	Indicate whether the software uses cryptography to protect any cryptographic keys (yes/no).		
	If "yes," **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that all cryptographic keys used to protect other cryptographic keys provide an effective key strength equal to or greater than the keys they protect.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
7.2.c Where any public keys are used by the system, the assessor shall examine vendor evidence and test the software to confirm that the vendor maintains an inventory of all cryptographic keys used by the software and that the authenticity of all public keys is maintained. Vendor evidence must identify: • Key label or name • Key location • Effective and expiration date • Key purpose/type • Key length	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Indicate whether the software uses public keys (yes/no). *If "no," skip to 7.2.d.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the documentation and evidence that contains the software vendor's inventory of all cryptographic keys used by the software.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that the authenticity of all public keys used in the software is maintained.		
7.2.d Where public or white-box keys are not unique per software instantiation the assessor shall examine vendor evidence and test the software to confirm that methods and procedures to revoke and/or replace such keys (or key pairs) exist.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software uses public or white-box keys that are not unique to each instance of the software.		
	Indicate whether any public or white-box keys are used by the software that are not unique to each software instance (yes/no).		
	If "yes," for each public or white-box keys used by the software that are not unique to each software instance, **describe** how the software (or the software vendor) revokes and/or replaces such keys (or key pairs).		
7.2.e Where the software relies upon external files or other data elements for key material (such as for public TLS certificates), the assessor shall examine vendor evidence to confirm that clear and sufficient guidance on how to install such key material in accordance with this standard—including details noting any security requirements for such key material—is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe any additional software tests performed to support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that the software relies upon external files or other data elements for cryptographic materials.		
	Indicate whether the software relies upon external files or other data elements for cryptographic key materials (yes/no).		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	If "yes," **identify** the documentation and evidence that contains the software vendor's guidance on how to install such key material.		
7.2.f Where public keys are used, the assessor shall examine vendor evidence and test the software to confirm that public keys manually loaded or used as root keys are installed and stored in a way that provides dual control (to a level that is feasible on the execution environment), preventing a single user from replacing a key to facilitate a man-in-the-middle attack, easy decryption of stored data, etc. Where complete dual control is not feasible (e.g., due to a limitation of the execution environment), the assessor shall confirm that the methods implemented are appropriate to protect the public keys.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that suggests the software uses manually loaded public keys or uses public keys as root keys.		
	Indicate whether the software uses any manually loaded public keys or uses public keys as root keys (yes/no). *If "no," skip to 7.2.g* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms the keys are stored in a way that provides for dual control.		
	Describe any circumstances that make the implementation of complete dual control over manually loaded or root keys infeasible. Also **describe** the methods implemented to protect the public keys in the absence of dual control.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
7.2.g The assessor shall examine vendor evidence and test the software to confirm that any secret and/or private keys are managed in a way that ensures split knowledge over the key, to a level that is feasible given the platform on which the software is executed. Where absolute split knowledge is not feasible, the assessor shall confirm that methods implemented are reasonable to protect secrets and/or private keys.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all secret and private keys are managed in a way that ensures split knowledge over each key.		
	Describe any circumstances that make the absolute split knowledge of secret or private keys infeasible. Also **describe** the methods implemented to protect the secret and private keys in the absence of split knowledge.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
7.2.h The assessor shall examine vendor evidence and test the software to confirm that methods are implemented to "roll" any keys at the end of their defined crypto-period that ensure the security of the sensitive data (both cryptographic keys and data secured through use of these keys) is in line with the requirements of this standard.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms the software vendor has defined crypto-periods for each of the cryptographic keys used for the protection of sensitive data.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that methods are implemented to "roll" cryptographic keys used for the protection of sensitive data at the end of their defined crypto-period.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
7.3 All random numbers used by the software are generated using only approved random number generation (RNG) algorithms or libraries. Approved RNG algorithms or libraries are those that meet industry standards for sufficient unpredictability (e.g., *NIST Special Publication 800-22*).			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
7.3.a The assessor shall examine vendor evidence to confirm that all random number generation methods implemented in the software: • Use at least 128 bits of entropy prior to the output of any random numbers from the random number generator. • 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms 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.				
	Describe what the assessor observed in the documentation and evidence 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.				
7.3.b Where the vendor is relying upon previous assessment of the random number generator, or source of initial entropy, the assessor shall examine the approval records of the previous assessment and test the software 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe any additional software tests performed in support this test requirement, including the tool(s)/method(s) used and the scope of each test.				
	Indicate whether the software relies upon a previous assessment of a random number generator or source of initial entropy to meet this control objective (yes/no). *If "no," skip to 7.3.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe the scope of the previous assessment (and approval).		
	Describe what the assessor observed in the documentation and evidence that confirms that all vendor claims pertaining to the random number generation function(s) used do not exceed the scope of evaluation or approval of those random number generation functions.		
7.3.c Where third-party software, platforms, or libraries are used for all or part of the random number generation process, the assessor shall examine current publicly available literature to confirm that there are no publicly known vulnerabilities or concerns with the software that may compromise its use for generating random values in the software under test. Where problems are known, but have been mitigated by the software vendor, the assessor shall examine vendor evidence and test the software to confirm that the vulnerabilities have been sufficiently mitigated. The assessor shall test the software to confirm that third-party software, platforms, or libraries are correctly integrated, implemented, and configured.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software relies on third-party software, platforms, or libraries for random number generation.		
	Indicate whether the software relies on third-party software, platforms, or libraries for all or part of the random number generation process (yes/no). *If "no," skip to 7.3.e.* *If "yes," complete the remaining reporting instructions for this test requirement and 7.3.d.*		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that third-party software, platforms, or libraries used as part of the random number generation process are implemented correctly.		
	Describe how the documentation, evidence, and software test results confirm that there are no known vulnerabilities or other weaknesses present in the third-party software, platforms, or libraries used as part of the random number generation process that would compromise the software's ability to generate sufficiently random values.		
	Describe any vulnerabilities that exist in the third-party software, platforms, or libraries that are used by the software as part of the random number generation process. Also **describe** the methods implemented in the software to mitigate those vulnerabilities.		
7.3.d The assessor shall examine vendor evidence and test the software to confirm that methods have been implemented to prevent or detect (and respond) the interception, or "hooking," of random number calls that are serviced from third-party software, or the platform on which the software is executed.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Summarize how the software mitigates the interception or "hooking" of random number calls to/from the third-party software, platforms, or libraries providing random number generation functions.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
7.3.e 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.*	**Identify** any additional documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test. Also **describe** how the assessor obtained at least 128MB of data output from each random number generator implemented by the software.		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicate that random number values cannot be statistically correlated.		
	Describe how the assessor confirmed that the methods used to generate the data output from the implemented random number generation function(s) ensure that the data is produced as it would be produced by the software during normal operation.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
7.4.a The assessor shall examine vendor 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, etc.) have entropy that meets the minimum effective strength requirements of the cryptographic primitives and keys.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.				
	Describe what the assessor observed in the documentation, evidence, and software test results that indicate that the methods used to generate cryptographic keys and other key material have entropy that meets the minimum effective strength requirements of the cryptographic primitives and keys. ***Note**: If sufficient entropy is not provided, then 7.4.c must be completed.*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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 vendor 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: • Any methods used for generating keys directly from a password/passphrase enforces 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 (e.g., a 32-hex-digit input field for an AES128 key). • The passphrase is passed through an industry-standard key-derivation function, such as PBKDF2 or bcrypt, which extends the work factor for any attempt to brute-force the passphrase value. The assessor shall confirm that a work factor of at least 10,000 is applied to any such implementation. *(continued on next page)*	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Indicate whether any cryptographic keys used by the software are generated through processes that require direct user interaction (yes/no). *If "no," skip to 7.4.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that the methods used to generate keys directly from a password/passphrase 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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that passwords/passphrases are passed through an industry-standard key-derivation function that provides a work factor of at least 10,000 for any attempt to brute-force the password/passphrase value.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
• Clear and sufficient guidance is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1 that any passphrase used must be: ○ Randomly generated itself, using a valid and secure random process: an online random number generator must not be used for this purpose. ○ Never implemented by a single person, such that one person has an advantage in recovering the clear key value; violating the requirements for split knowledge.	**Identify** the documentation and evidence that contains the software vendor's guidance on using passwords/passphrases that are randomly generated using a valid and secure random process.		
	Identify the documentation and evidence that contains the software vendor's guidance on using passwords/passphrases that do not violate requirements for split knowledge.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
7.4.c Where any third-party software or platforms are relied upon by the software and do not meet the entropy requirements, the assessor shall examine vendor evidence and test the software to confirm that sufficient mitigations are implemented, and that clear and sufficient guidance on the secure configuration and usage of these software components is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Indicate whether any instances were found where third-party software, platforms, or libraries used as part of the random number generation process could not produce sufficient entropy (yes/no). *If "no," skip to 8.1.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that appropriate mitigations are implemented to compensate for the lack of sufficient entropy.		
	Identify the documentation and evidence that contains the software vendor's guidance on securely configuring and using third-party software, platforms, or libraries that are part of the random number generation process.		

Secure Software Operations

The software vendor facilitates secure software operation.

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 8: Activity Tracking All software activity involving critical assets is tracked.					
8.1 All access attempts and usage of critical assets is tracked and traceable to a unique individual. ***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** ☐	**N/A** ☐	**Not in Place** ☐
8.1.a The assessor shall examine vendor evidence and test the software to confirm that all access attempts and usage of critical assets are tracked and traceable to a unique identification for the person, system, or entity performing the access.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all access attempts and use of critical assets are tracked and traced to a unique identification for the person, system, or entity accessing the critical assets.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
8.2 All activity is captured in sufficient and necessary detail to accurately describe what specific activities were performed, who performed them, the time they were performed, and which critical assets were impacted.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
8.2.a The assessor shall examine vendor 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 functionality	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.				
	For each of the activities identified in this test requirement, **describe** how the software captures each activity in its activity logs or other activity tracking mechanism(s).				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
8.2.b The assessor shall examine vendor evidence and test the software to confirm that the tracking method(s) implemented provide: • A unique identification for the person, system, or entity performing the access • A timestamp for each tracked event • Details on what critical asset has been accessed	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe how the information identified in this test requirement is presented in the software activity logs or other activity tracking mechanism(s).		
8.2.c The assessor shall test the software to confirm that sensitive data is not directly recorded in the tracking data.	**Identify** any additional documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in any documentation, evidence, and software test results that confirms that sensitive data is not recorded in activity logs or in the output of other activity tracking mechanisms.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
8.3 The software supports secure retention of detailed activity records.			**In Place**	**N/A**	**Not in Place**
			☐	☐	☐
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 vendor evidence and test the software to confirm that the protection methods are implemented to protect completeness, accuracy, and integrity of the activity records.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software manages activity records.				
	Indicate whether activity records are managed by the software (yes/no). *If "no," skip to 8.3.b.* *If "yes," complete the remaining reporting instructions for this test requirement.*				
	Describe the protection methods implemented by the software to protect the integrity of activity records.				
	Describe how the protection methods for ensuring the integrity of activity records mitigate the risk of unauthorized modification of the activity records.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
8.3.b Where the software utilizes other systems for maintenance of tracking data, such as a log server, the assessor shall examine vendor evidence to confirm that clear and sufficient guidance on the correct and complete setup and/or integration of the software with the log storage system is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1. 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software uses or supports the use of external systems for storing or maintaining activity tracking data.		
	Indicate whether the software uses or supports the use of other systems for storing or maintaining activity tracking data (yes/no). *If "no," skip to 8.4.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe the methods implemented by the software to secure the authenticity of activity tracking data during transmission to third-party or external activity tracking or log storage system(s).		
	Identify the documentation and evidence that contains the software vendor's guidance on how to securely configure the integration of the software with third-party or external activity tracking and/or log storage system(s).		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
8.4 The software handles failures in activity-tracking mechanisms such that the integrity of existing activity records is preserved.			In Place ☐	N/A ☐	Not in Place ☐
8.4.a The assessor shall examine vendor evidence and test the software to confirm that failure of the activity tracking system does not violate the integrity of existing records. The assessor shall explicitly confirm 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. • Where possible the software applies 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that the software does not overwrite any tracking data upon a restart of the software, and each new start only appends to existing datasets or creates a new tracking dataset.				
	Where unique dataset names are relied upon by the software for maintaining the integrity between execution instances, **describe** the methods implemented in the software to prevent other software (or instance of the same software) from overwriting or rendering invalid any existing data sets.				
	Describe any conditions that exist that make it difficult for the software to apply file privileges to assist with maintaining the integrity of the activity tracking data set and any additional mitigations implemented to ensure the integrity of activity tracking data.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
8.4.b The assessor shall examine vendor evidence, including source code, and shall test the software, including (wherever possible): • 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 (e.g., by using media that has insufficient available space). 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 put in place to prevent such scenarios from affecting the integrity of the tracking records.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, source code, and software test results that confirms whether attempts to circumvent or overwrite activity tracking mechanisms and data are possible.		
	Indicate whether any of the tests specified in this test requirement could not be performed or did not produce the expected result (yes/no). *If "no," skip to 9.1.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	For each of the software tests that could not be performed or do not produce the expected result, **describe** the factors that prevent such tests from producing results as expected and the additional protections implemented to protect the integrity of activity tracking records.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 9: Attack Detection Attacks are detected, and the impacts/effects of attacks are minimized.					
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** ☐	**N/A** ☐	**Not in Place** ☐
9.1.a The assessor shall examine vendor evidence and test the software to confirm that, where possible, the software implements a method to validate the integrity of its own executable and any configuration options, files, and datasets that it relies upon for operation (such that unauthorized, post-deployment changes can be detected). Where the execution environment prevents this, the assessor shall examine vendor evidence and current publicly available literature on the platform and associated technologies to confirm that there are indeed no methods for validating authenticity. The assessor shall then test the software to confirm controls are implemented to minimize the associated risk.	**Identify** the documentation and evidence examined for this test requirement.				
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.				
	Describe the method(s) implemented by the software to validate the integrity and authenticity of its own files.				
	Indicate whether the execution environment or other factors prevent the software from validating the integrity of its own files (yes/no). *If "no," skip to 9.1.b.* *If "yes," complete the remaining reporting instructions for this test requirement.*				
	Describe how and to what extent the assessor attempted to identify other methods for validating the authenticity of software executables, configuration files, and datasets.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe the additional controls implemented by the software to protect the integrity of the software's executables, configuration options, files, and datasets that it relies upon for operation to minimize the associated risk and to compensate for the lack of integrity checking mechanisms.		
9.1.b The assessor shall examine vendor 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). The assessor shall confirm what action the software takes upon failure of these checks and confirm that the processing of sensitive data is halted until this problem is remediated.	**Identify** the documentation and evidence examined for this test requirement.		
	Describe the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe the frequency with which integrity values used by the software and dataset(s), upon which the software relies upon for secure operation, are checked.		
	Describe the actions the software takes upon the failure of such integrity checks.		
9.1.c Where cryptographic primitives are used by any anomaly-detection methods, the assessor shall examine vendor evidence and test the software to confirm that cryptographic primitives are protected.	**Identify** the documentation and evidence examined for this test requirement.		
	Describe the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software testing results that confirms whether the software uses cryptographic primitives to detect anomalies.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Indicate whether cryptographic primitives are used by the software to detect anomalies (yes/no).		
	If "yes," **describe** what the assessor observed in the documentation, evidence, and software testing results that confirms that protection mechanisms are implemented to protect cryptographic primitives, and that those protections are appropriate for their intended purpose.		
9.1.d Where stored values are used by any anomaly-detection methods, the assessor shall examine vendor evidence and test the software to confirm that these values are considered sensitive data and protected accordingly.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation and evidence that confirms whether stored values are used by the software to detect anomalies.		
	Indicate whether stored values are used by the software for to detect anomalies (yes/no).		
	If "yes," **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that protection mechanisms are implemented to protect stored values, and that the protection mechanisms are appropriate for their intended purpose.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
9.1.e Where configuration or other dataset values can be modified by the software during execution, the assessor shall examine vendor 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tool(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and results of the software tests that confirms whether configuration or other data set values can be modified by the software during execution.		
	Indicate whether configuration or other dataset values (relied upon by the software for operation) can be modified by the software during execution (yes/no). *If "no," skip to 9.1.f.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe the integrity protections implemented to protect configuration or other dataset values from modification during software execution.		
	For each of the integrity protections implemented, **describe** how the implementation allows for updates during execution, while ensuring that the integrity of the values can be validated after the update.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
9.1.f The assessor shall examine vendor 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 (e.g., input rate limiting).	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe each of the software tests performed in support of this test requirement, including the tools(s)/method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that controls are implemented to prevent brute-force attacks on account, password, or cryptographic-key input fields, and that the controls are appropriate for their intended purpose.		

Secure Software Lifecycle Management

The software vendor implements secure software lifecycle management practices.

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 10: Threat and Vulnerability Management The software vendor identifies, assesses, and manages threats and vulnerabilities in its payment software.					
10.1 Software threats and vulnerabilities are identified, assessed, and addressed.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
10.1.a The assessor shall examine vendor evidence to confirm that the vendor identifies common methods for attack against the software product. This may include platform-level, protocol-level, and/or language-level attacks.	**Identify** the documentation and evidence examined that identifies and describes the attack methods applicable to the software.				
10.1.b The assessor shall examine vendor evidence to confirm that the list of common attacks is valid for the software the vendor has produced and shall note where this does not include common attack methods detailed in industry-standard references such as OWASP and CWE lists.	**Describe** what the assessor observed in the documentation and evidence examined in 10.1.a that indicates that the software vendor has conducted a reasonably comprehensive assessment of the common software attack methods applicable to the software and the software's susceptibility to them.				
10.1.c The assessor shall examine vendor evidence to confirm that mitigations against each identified attack vector exists, and that the vendor's software release process includes validation of the existence of these mitigations.	**Identify** the documentation and evidence examined in support of this test requirement, including the documentation and evidence examined in 10.1.a.				
	Describe what the assessor observed in the documentation and evidence that confirms that protection mechanisms are implemented to mitigate each of the common attacks applicable to the software, and that the mitigations are appropriate for their intended purpose.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
10.2 Vulnerabilities in the software and third-party components are tested for and fixed prior to release.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
10.2.a The assessor shall examine vendor evidence to confirm that the software vendor has implemented robust testing processes throughout the software lifecycle to validate the mitigations used to secure the software against attacks outlined in the vendor threat model and vulnerability assessment.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor has implemented testing processes to verify that all protection mechanisms implemented in the software to mitigate each of the potential attacks identified in 10.1.a remain in place and operate effectively.				
	Describe what the assessor observed in the documentation and evidence that confirms that such processes are implemented throughout the entire software lifecycle.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
10.2.b The assessor shall examine evidence, including documented testing processes and output of several instances of the testing, as performed on the software under evaluation 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 tools for security testing that are appropriate for detecting applicable vulnerabilities and are suitable for the software architecture, development languages, and frameworks used in the development of the software. • Accounts for the entire code base, including detecting 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 retesting of the software.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe the automated tools used as part of the vendor's testing process to detect vulnerabilities in software code and during execution, and why they are appropriate for the software architecture and the software development languages and frameworks in use.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor's testing process accounts for the entire code base, including third-party, open-source, or other shared components and libraries.		
	Describe what the assessor observed in the documentation and evidence that indicates that the software vendor's testing process reasonably accounts for all common vulnerabilities and attack methods applicable to the software.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor's testing process demonstrates a history of successfully finding software vulnerabilities and remediating them prior to software release.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
10.2.c Where vendor evidence shows the release of software with known vulnerabilities, the assessor shall examine vendor evidence to confirm that: • The vendor implements an industry-standard vulnerability-ranking system (such as CVSS) that allows for the categorization of vulnerabilities. • For all vulnerabilities, the vendor provides a remediation plan—it is unacceptable for a known vulnerability to remain unmitigated for an indefinite period.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Summarize the software vendor's vulnerability ranking/categorization scheme and how it aligns with other industry-standard schemes.		
	Describe how the software vendor's process ensures vulnerabilities do not remain unmitigated indefinitely.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective 11: Secure Software Updates The software vendor facilitates secure software releases and updates.					
11.1 Software updates to fix known vulnerabilities are made available to stakeholders in a timely manner.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
11.1.a The assessor shall examine vendor evidence to confirm that: • Reasonable criteria exist for releasing software updates to fix security vulnerabilities. • Security updates are made available to stakeholders in accordance with defined criteria.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Summarize the software vendor's criteria for how and how often the vendor releases software updates to fix security vulnerabilities.				
	Describe the assessor's rationale for why the software vendor's security update release criteria are reasonable given the software's intended purpose and function, and the critical assets maintained by the software.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor makes security updates available to stakeholders in accordance with its own defined security update release criteria and does not make exceptions on a regular basis.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
11.1.b For a sample of vendor software updates, the assessor shall examine vendor evidence, including update-specific security-testing results and details, to confirm security fixes have been made available to stakeholders in accordance with defined criteria. Where updates were not provided in accordance with defined criteria, such instances are be reasonably justified by the vendor.	**Identify** the documentation and evidence examined in support of this requirement.		
	Identify the software update sample selected in support of this test requirement.		
	Indicate whether any evidence was obtained that suggests the software vendor did not provide security fixes to stakeholders in accordance with its own defined criteria (yes/no).		
	If "yes," for each instance identified **describe** the vendor's justification for not providing security fixes, and why the assessor considers each exception reasonable given the risk posed by the continued existence of known vulnerabilities in the software.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
11.2 Software releases and updates are delivered in a secure manner that ensures the integrity of the software and its code.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
11.2.a The assessor shall examine vendor evidence to confirm that the method by which the vendor releases software updates ensures the integrity of the software and its code during transmission and install. Where user instructions are required to validate the integrity of the code, the assessor shall confirm that clear and sufficient guidance to enable the process to be correctly performed is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe any additional software tests performed in support of this test requirement, including the tool(s) or method(s) used and the scope of each test.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that the software vendor's methods for delivering software updates protect the integrity of the software and its code during transmission and installation (or implementation).				
	Indicate whether the software requires user interaction to validate the integrity of the software update code (yes/no).				
	If "yes," **identify** the documentation and evidence that contains the software vendor's guidance on how to verify the integrity of software update code.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
11.2.b Where the integrity method implemented is not cryptographically secure (such as through the use of digital signatures), the assessor shall examine vendor 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).	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms whether the software provides software integrity validation methods that are cryptographically insecure.		
	Indicate whether the methods to protect the integrity of software update code are cryptographically insecure (yes/no).		
	If "yes," **describe** how the documentation and evidence demonstrates that the software distribution methods provide a suitable chain of trust.		
11.2.c The assessor shall examine vendor evidence to confirm that the software vendor informs users of the software updates, and that clear and sufficient guidance on how they may be obtained and installed is provided in the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor informs uses and other stakeholders when security updates are available.		
	Identify the documentation and evidence that contains the software vendor's guidance on how to obtain and install security updates.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
11.2.d The assessor shall examine vendor evidence to confirm the vendor has a process for informing users of the software of known vulnerabilities that have not yet been patched by a new version of the software. This includes vulnerabilities that may exist in third-party software and libraries used by the vendor's software product. The assessor shall confirm that this process includes providing the users with suggested mitigations for any such vulnerabilities.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides users with mitigation techniques when vulnerabilities are detected in the software and a security patch cannot be provided in a timely manner.		
11.2.e The assessor shall examine vendor evidence to confirm the 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 security.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor's update mechanisms cover all software, configuration files, and metadata used by the software for security purposes or could affect the security of the software.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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.					
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** ☐	**N/A** ☐	**Not in Place** ☐
12.1.a The assessor shall examine vendor evidence to confirm that the vendor creates and provides, to all stakeholders, clear and sufficient guidance to allow for the secure installation and use of the software.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Summarize how the software vendor makes implementation guidance available to all stakeholders, whether it's provided as a single document, multiple documents, a series of independent notifications, or content posted on the software vendor's website, and so on.				
12.1.b The assessor shall examine vendor 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). *(continued on next page)*	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides stakeholders with guidance on how to install and configure the software, including any third-party software required.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides stakeholders with instructions on how to securely configure the platform and/or environment in which the software is to execute, including configuring any platform parameters or other resources upon which the software relies.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
• Includes instructions for key management (e.g., use of keys, how keys are distributed, loaded, removed, changed, destroyed, etc.) • 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. • 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 reasonable justification exists for why this is the case and confirm that it agrees with their understanding and the results of their testing of the software.	**Describe** what the assessor observed in the documentation and evidence that confirms that the software vendor provides stakeholders with instructions on how to manage all cryptographic keys used by the software, including how those keys are to be managed; that is, distributed, loaded, removed, changed, or destroyed, etc.).		
	Describe what the assessor observed in the documentation and evidence that confirms that users are never instructed to disable security settings or parameters in the installed environment that support software operation.		
	Describe what the assessor observed in the documentation and evidence that confirms that users are never instructed to execute the software in a privileged mode higher than the minimum privilege necessary for software operation.		
	Describe what the assessor observed in the documentation and evidence that confirms that the guidance provided to stakeholders clearly identifies the version(s) of the software to which it applies.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor identifies all requirements within this standard that are not applicable and provides reasonable explanations for why each requirement is not applicable.		

Account Data Protection

The confidentiality of Account Data is protected.

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective A.1: Sensitive Authentication Data Sensitive authentication data is not retained after authorization.					
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** ☐	**N/A** ☐	**Not in Place** ☐
A.1.1.a For each instance of sensitive authentication data identified in Control Objective 1, the assessor shall test the software, including generation of error conditions and log entries, and usage of forensic tools and/or methods, to identify all potential storage locations and to confirm that the software does not store sensitive authentication data after authorization. This includes temporary storage (such as volatile memory), semi-permanent storage (such as RAM disks), and non-volatile storage (such as magnetic and flash storage media).	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software stores sensitive authentication data after authorization.				
A.1.1.b Where sensitive authentication data is stored after authorization, the assessor shall examine vendor evidence to confirm the software is intended only for use by issuers or organizations that support issuing services.	Based on the documentation and evidence reviewed, and software testing performed in A1.1.a, **indicate** whether any evidence was obtained that suggests that the software stores sensitive data after authorization (yes/no).				
	If "yes," **Describe** what the assessor observed in the documentation and evidence that indicates that the software is intended only for use by issuers or organizations that support issuing services.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective A.2: Cardholder Data Protection Stored cardholder data is protected.					
A.2.1 The software vendor provides guidance to customers regarding secure deletion of cardholder data after expiration of the customer-defined retention period.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
A.2.1 The assessor shall examine the instructions prepared by the software vendor and confirm the documentation includes the following guidance for customers, integrators, and resellers: • A list of all locations where the software stores cardholder data. • Instructions on how to securely delete cardholder data stored by the payment software, including data stored on underlying software or systems (such as OS, databases, etc.). • Instructions for configuring the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture or retention of cardholder data—for example, system backup or restore points.	**Identify** the documentation and evidence in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders (including customers, integrators, and resellers) that identifies and describes all locations within the software and its execution environment where cardholder data is stored.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders (including customers, integrators, and resellers) on how to securely delete cardholder data wherever it is stored.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders (including customers, integrators, and resellers) on how to configure the software or underlying systems to prevent the inadvertent capture or retention of cardholder data.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
A.2.2 The software masks the PAN such that only a maximum of the first six and last four digits are displayed by default.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
A.2.2.a The assessor shall examine vendor evidence, including the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1, to confirm the guidance includes the following instructions for customers and integrators/resellers: • Details of all instances where PAN is displayed. • Confirmation that the payment software masks PAN to display a maximum of the first six and last four digits by default on all displays. • Instructions for how to configure the software to display more than the first six/last four digits of the PAN (includes displays of the full PAN).	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders that identifies all locations within the software or underlying systems where PAN is displayed.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders that instructs them to mask all displays of PAN to a maximum of the first six and last four digits by default, and how to do so.				
	Based on the documentation and evidence, **indicate** whether the software supports the full display of PAN (yes/no).				
	If "yes," **Describe** what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders on how to properly configure the software to display more than the first six and last four digits of the PAN.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
A.2.2.b The assessor shall test the software to confirm that all displays of PAN are masked by default.	**Identify** any additional documentation and evidence in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that indicates that all displays of PAN are masked to a maximum of the first six and last four digits by default.		
A.2.2.c The assessor shall examine vendor evidence and test the software to confirm that for each instance where the PAN is displayed, the instructions for displaying more than the first six/last four digits are accurate.	**Identify** any additional documentation and evidence in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that by following the software vendor's guidance on configuring PAN masking, the software only displays first six and last four digits of the PAN.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
A.2.3 Render the PAN 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** ☐	**N/A** ☐	**Not in Place** ☐
A.2.3.a The assessor shall examine vendor evidence, including the software vendor's implementation guidance made available to stakeholders per Control Objective 12.1 to verify the guidance includes the following: • Details of any configurable options for each method used by the software to render cardholder data unreadable, and instructions on how to configure each method for all locations where cardholder data is stored by the payment software. • A list of all instances where cardholder data may be output for the customer to store outside of the payment application, and instructions that the customer is responsible for rendering the PAN unreadable in all such instances. • Instruction that if debugging logs are ever enabled (for example, for troubleshooting purposes) and they include the PAN, they must be protected, disabled as soon as troubleshooting is complete, and securely deleted when no longer needed.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders that identifies all available options to render cardholder data unreadable, and that instructions are also provided to securely configure those options.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders that identifies all instances where cleartext cardholder data is output by the software and instructs stakeholders that they are responsible for rendering such instances of PAN unreadable.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders instructing them that they are responsible for ensuring that PAN remains protected wherever debugging logs are enabled.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
A.2.3.b The assessor shall test the software to confirm that the method used to protect the PAN, including the encryption algorithms (if applicable), and verify that the PAN is rendered unreadable using any of 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.*	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that PAN is rendered unreadable wherever it is stored persistently.		
	Identify the documentation and evidence examined in support of this test requirement.		
	Describe any additional software tests performed in support of this test requirement, including the tool(s) or method(s) used and the scope of each test.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software creates both tokenized and truncated versions of the same PAN.		
	Where the software creates both tokenized and truncated versions of the same PAN, **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that tokenized and truncated versions of the PAN cannot be correlated to reconstruct the original PAN.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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 test the software, including examining a sample of generated files, such as those generated on removable media (for example, back-up tapes), to confirm that the PAN is rendered unreadable.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms whether the software generates files for use outside of the software.		
	Where the software creates or generates files for use outside of the software, **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that PAN is either excluded from all such files, or it is rendered unreadable by the software.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
A.2.3.e If the software vendor stores the 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 vendor evidence and test the software to confirm that the PAN is rendered unreadable in accordance with this requirement.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Indicate whether any evidence was found through the documentation, evidence, or software test results that suggests that the software vendor stores PAN on vendor systems (yes/no).		
	If "yes," **describe** what the assessor observed in the documentation, evidence, and software test results that confirms that PAN is rendered unreadable wherever and whenever it is stored on vendor systems.		

Terminal Software Security

Terminal software protects account data from unauthorized disclosure and ensures the underlying payment terminal's security features, functions and characteristics are not circumvented or otherwise rendered ineffective.

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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.					
B.1.1 The software vendor maintains documentation that describes all software components, interfaces, and services provided or used by the software.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.1.1 The assessor shall examine all relevant documentation and evidence necessary to confirm that the software vendor maintains documentation describing 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.	**Identify** the documentation and evidence examined that identifies and describes all third-party and open-source components, external services, and Application Programming Interfaces (APIs) used by the software.				
	Identify the documentation and evidence that identifies and describes all User Interfaces (UI) and APIs provided or made accessible by the software.				
	Identify any other documentation or evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence to conclude that all third-party and open-source components, external services, and APIs used by the software are documented.				
	Describe what the assessor observed in the documentation and evidence to conclude that all UI's and APIs provided or made accessible by the software are documented.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
B.1.2.a The assessor shall examine all relevant documentation and evidence necessary to confirm that the software vendor maintains documentation describing 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.	**Identify** the documentation and evidence examined that identifies and describes the sensitive data that is stored, processed, or transmitted by the software. ***Note****: If this documentation is the same as the documentation and evidence examined in the testing for Core Requirements 1.1 or 1.2, note that here in addition to specifying the document name(s) or reference number(s).*				
	Identify the documentation and evidence examined that identifies and describes the locations where sensitive data is stored. ***Note****: If this documentation is the same as the documentation and evidence examined in the testing for Core Requirements 1.1 or 1.2, note that here in addition to specifying the document name(s) or reference number(s).*				
	Identify the documentation and evidence examined that describes how sensitive data is securely deleted from storage when no longer needed. ***Note****: If this documentation is the same as the documentation and evidence examined in the testing for Core Requirements 1.1 or 1.2, note that here in addition to specifying the document name(s) or reference number(s).*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
B.1.2.b The assessor shall examine all relevant documentation and evidence necessary to confirm that the software vendor maintains documentation describing 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.	**Identify** the documentation and evidence examined that identifies and describes all software functions that handle sensitive data. ***Note**: If this documentation is the same as the documentation and evidence examined in the testing for Core Requirements 1.1 or 1.2, note that here in addition to specifying the document name(s) or reference number(s).*		
	Identify the documentation and evidence examined that identifies and describes all inputs and outputs for each software function that handles sensitive data.		
	Identify the documentation and evidence examined that identifies and describes all possible error conditions for each software function that handles sensitive data.		
	Identify the documentation and evidence examined that identifies and describes the cryptographic algorithms and modes of operation used and supported for each instance where cryptography is used to protect sensitive data.		
	Identify the documentation and evidence examined that identifies and describes how cryptographic keys are managed for each instance where cryptography is used to protect sensitive data.		
	Identify any other documentation and evidence examined in support of this test requirement.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
B.1.3 The software vendor maintains documentation that describes all configurable options that can affect the security of sensitive data.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.1.3 The assessor shall examine all relevant documentation and evidence necessary to confirm that the software vendor maintains documentation describing 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.	**Identify** the documentation and evidence examined that identifies and describes all configurable options that enable access to sensitive data.				
	Identify the documentation and evidence examined that identifies and describes all configurable options that enable modification of mechanisms used to protect sensitive data.				
	Identify the documentation and evidence examined that identifies and describes all remote access features, functions, and parameters provided or made available by the software.				
	Identify the documentation and evidence examined that identifies and describes all remote update features, functions, and parameters provided or made available by the software.				
	Identify the documentation and evidence examined that describes the default settings for each configurable option.				
	Identify any other documentation and evidence examined in support of this test requirement.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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.					
B.2.1 The software is intended for deployment and operation on payment terminals (i.e., PCI-approved POI devices).			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.2.1 The assessor shall examine all relevant software documentation and evidence necessary to determine the payment terminals upon which the software is to be deployed. For each of the payment terminals identified in the software documentation 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)	**Identify** the documentation and evidence examined that identifies the POI devices supported by the software.				
	Identify any other documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software is intended for deployment on PCI-approved POI devices.				
	Describe what the assessor observed in the documentation and evidence that confirms that the device characteristics of the POI devices supported by the software match the device characteristics specified in the *PCI SSC's List of Approved PTS Devices.*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
B.2.2.a The assessor shall examine all relevant software documentation and source code necessary to determine whether the software supports external communications.	**Identify** the documentation and evidence examined that confirms whether the software supports external communications.				
	Describe how and the extent to which the source code was examined to determine whether the software support supports external communications.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms whether the software supports external communications.				
	Indicate whether the software supports external communications (yes/no). *If "no," skip to B.2.3.* *If "yes," complete the reporting instructions for test requirements B.2.2.b through B.2.2.2.*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Identify the external communication methods included in the payment terminal's PTS POI device evaluation.		
	Indicate whether there are any discrepancies between the list of external communication methods used by the software and the list of PCI-approved external communication methods provided by the payment terminal. (yes/no). *If "no," skip to B.2.2.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe each of the discrepancies between the external communication methods supported by the software and those included in the payment terminal's PTS POI device evaluation.		
	For each of the noted discrepancies, **describe** the assessor's rationale for why the discrepancy does not violate the control objective.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
B.2.2.c The assessor shall examine all relevant software documentation and source code necessary 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 (i.e., its own IP stack).	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which the source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms the software only uses the PCI-approved external communication methods included in the payment terminal's PTS POI device evaluation and does not implement its own external communication methods (that is, its own IP stack).				
B.2.2.1 Where the software relies on the Open Protocols features of the payment terminal, the software is developed in accordance with the payment terminal vendor's security guidance/policy.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms whether the software relies on the Open Protocols features of the payment terminal.				
	Indicate whether the software relies on the Open Protocols features of the payment terminal (yes/no). *If "no," skip to B.2.3.* *If "yes," complete the remaining reporting instructions for test requirements B.2.2.1 through B.2.2.2.*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Describe what the assessor observed in the documentation and evidence that confirms that the software is developed in accordance with the payment terminal vendor's security guidance/policy.				
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, and IP services.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.2.2.2 The assessor shall examine all relevant software documentation and 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	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which the source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that the software does not circumvent, bypass, or add additional services or protocols to the Open Protocols approved as part of the payment terminal's PCI PTS device evaluation.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
B.2.3.a The assessor shall examine all relevant software documentation and source code necessary to determine whether the software facilitates 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:	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which the source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code that determines whether the software supports the encryption of sensitive data.				
	Indicate whether the software supports the encryption of sensitive data (yes/no). *If "no," skip to B.2.4.* *If "yes," complete the reporting instructions for test requirements B.2.3.b through B.2.3.d.*				
B.2.3.b The assessor shall examine all relevant payment terminal documentation—including payment terminal vendor security guidance/policy—necessary to determine which encryption methods are provided by the payment terminal.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Identify each of the encryption methods provided by the payment terminal.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
B.2.3.c The assessor shall examine all relevant software documentation and source code necessary 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe how and the extent to which the source code was examined in support of this test requirement.		
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that the software does not bypass or render ineffective any encryption methods provided by the payment terminal.		
B.2.3.d Where the software facilitates 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 all relevant software documentation and source code necessary 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe how and the extent to which source code was examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms whether the payment terminal is required to provide approved encryption methods as part of its PCI PTS POI device evaluation.		
	Indicate whether the payment terminal is required to provide approved encryption methods as part of its PCI PTS POI device evaluation (yes/no). *If "yes," skip to B.2.4.* *If "no," complete the remaining reporting instructions for this test requirement.*		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Describe what the assessor observed in the software documentation, evidence, and source code that confirms that the encryption methods used or implemented by the software for encrypting sensitive data provide strong cryptography in accordance with Control Objectives 7.1 and 7.2.				
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** ☐	**N/A** ☐	**Not in Place** ☐
B.2.4.a The assessor shall examine all relevant software documentation and source code necessary to determine whether the software requires random values to be generated for any cryptographic operations involving sensitive data or sensitive functions.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which the source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code examined that confirms whether the software requires random number values for cryptographic operations involving sensitive data or sensitive functions.				
	Indicate whether the software requires random number values for cryptographic operations involving sensitive data or sensitive functions (yes/no). *If "no," skip to B.2.5.* *If "yes," complete the reporting instructions for test requirements B.2.4.b through B.2.4.c.*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
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—necessary to determine all of the random number generation functions included in the payment terminal's PTS device evaluation.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Indicate whether there are any discrepancies between the list of random number generation functions used by the software and the list of PCI-approved random number generation functions provided by the payment terminal (yes/no). *If "no," skip to B.2.4.c.* *If "yes," complete the remaining reporting instructions for this test requirement.*		
	Identify the discrepancies found between the random number functions used by the software and those included in the payment terminal's PTS POI device evaluation.		
	For each of the noted discrepancies, **describe** the assessor's rationale for why the discrepancy does not violate the parent control objective.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
B.2.4.c The assessor shall examine all relevant software documentation and source code necessary 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).	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe how and the extent to which source code was examined in support of this test requirement.		
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that the software only uses the PCI-approved random number generation functions included in the payment terminal's PCI PTS POI device evaluation and does not implement its own random number generation functions.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
B.2.5 The software does not facilitate, 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** ☐	**N/A** ☐	**Not in Place** ☐
B.2.5.a The assessor shall examine all relevant software documentation and source code necessary 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which the source code was examined in support of this test requirement.				
	Identify all discrepancies found between the logical interfaces identified through documentation and evidence reviews and the logical interfaces identified through source code reviews.				
	For each of the noted discrepancies, **describe** the software vendor's justification for why the discrepancy exists and the assessor's rationale for why the discrepancy is considered acceptable.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
B.2.5.b The assessor shall examine all relevant software documentation and source code necessary to confirm that the software does not facilitate sharing of clear-text account data directly with other software through its own logical interfaces.	**Describe** what the assessor observed in the documentation, evidence, and source code in B.2.5.a that indicates that the software does not support sharing of clear-text account data directly with other software through its own logical interfaces.		
B.2.5.c The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.) the assessor shall test the software using all software functions that handle account data to confirm that the software does not facilitate the sharing of clear-text account data directly with other software through its own logical interfaces.	**Describe** each of the tests performed in support of this test requirement, including the tool(s) or method(s) used and the scope of each test.		
	Describe what the assessor observed in the software testing results that confirms that the software does not facilitate the sharing of cleartext account data directly with any other software through its own logical interfaces.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
B.2.6.a The assessor shall examine all relevant software documentation and source code necessary 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 software vendor's implementation 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 software vendor's implementation guidance for secure integration with such shared resources is in accordance with the payment terminal vendor's security guidance/policy.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms whether the software connects to and/or uses any shared resources provided by the payment terminal.				
	Indicate whether the software connects to or uses any shared resources provided by the payment terminal (yes/no). *If "no," skip to B.2.7.* *If "yes," complete the remaining reporting instructions for this test requirement and test requirement B.2.6.b.*				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders on how to configure the software and securely integrate with each of the shared resources provided by the payment terminal.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor's guidance is in accordance with the payment terminal vendor's security guidance/policy.				
B.2.6.b The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.) 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.	**Identify** any additional documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that the software's connection to and use of any shared resources provided by the payment terminal are handled securely.				
B.2.7 The software does not bypass or render ineffective any application segregation enforced by the payment terminal.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.2.7.a The assessor shall examine all relevant payment terminal documentation—including the payment terminal vendor's security guidance/policy—necessary to determine whether and how application segregation is enforced by the payment terminal.	**Identify** the documentation and evidence examined in support of this test requirement.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
B.2.7.b The assessor shall examine all relevant software documentation and source code necessary 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which source code was examined in support of this test requirement.				
	Describe what the assessor observed in documentation, evidence, and source code that confirms that the software does not include functions that would enable it to bypass or defeat any device-level application segregation controls provided by an underlying payment terminal.				
B.2.8 All software files are cryptographically signed to facilitate cryptographic authentication of the software files by the payment terminal firmware.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.2.8.a The assessor shall examine the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1 to confirm it includes detailed instructions for how to cryptographically sign the software files in a manner that facilitates the cryptographic authentication of all such files by the payment terminal.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders on how to cryptographically sign software files in a manner that supports cryptographic authentication of all such files by an underlying payment terminal's firmware.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
B.2.8.b The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.) the assessor shall confirm that all software files are cryptographically signed in a manner that facilitates the cryptographic authentication of all software files.	**Identify** any additional documentation and evidence examined in support this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and software test results that confirms that all software files are cryptographically signed in a manner that supports the cryptographic authentication of all software files by an underlying payment terminal's firmware.		
B.2.8.c Where the software supports the loading of files outside of the base software package(s), the assessor shall determine whether each of those files is cryptographically signed in a manner that facilitates 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 each such files does not adversely affect the security of the software or the underlying payment terminal.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe how and the extent to which source code was examined to support this test requirement.		
	Describe what the assessor observed in the documentation, evidence, and source code that confirms whether the software supports the loading of files outside of the base software package(s).		
	Indicate whether evidence was found to suggest that the software supports the loading of files outside of the base software package(s) (yes/no). *If "no," skip to B.2.9.* *If "yes," complete the remaining reporting instructions for this test requirement.*		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and source code that confirms whether external files loaded by the software are cryptographically signed in a manner that supports the cryptographic authentication of those files by an underlying payment terminal's firmware.		
	Where files were found that were not or could not be cryptographically signed, **describe** the assessor's rationale for why the inability to cryptographically sign and authenticate such files does not adversely affect the security of the software or an underlying payment terminal.		
B.2.8.d The assessor shall examine all relevant software documentation and source code necessary 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 software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.) the assessor shall confirm that all EMV Certification Authority Public Keys are cryptographically signed in a manner that facilitates the cryptographic authentication of those files by the payment terminal.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe how and the extent to which source code was examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the documentation, evidence, and source code that confirms whether the software supports EMV® payment transactions.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Describe what the assessor observed in the documentation, evidence, source code, and software testing results that confirms that all EMV Certification Authority Public Keys are cryptographically signed in a manner that supports the cryptographic authentication of those files by the payment terminal.				
B.2.9 The integrity of software prompt files is protected in accordance with Control Objective B.2.8.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.2.9.a The assessor shall examine all relevant software documentation and source code necessary 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms whether the software supports the use of data entry prompts and/or prompt files.				
	Indicate whether the software supports the use of data entry prompts and/or prompt files (yes/no). *If "no," skip to B.3.1.* *If "yes," complete the remaining reporting instructions for test requirements B.2.9.b through B.2.9.c.*				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
B.2.9.b The assessor shall examine the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1 to confirm it includes detailed instructions for directing software stakeholders to cryptographically sign all prompt files in a manner that facilitates the cryptographic authentication of all such files in accordance with B.2.8.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides guidance to stakeholders on how to cryptographically sign all prompt files in a manner that supports the cryptographic authentication of those files in accordance with Control Objective B.2.8.		
B.2.9.c The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.) the assessor shall confirm that all prompt files are cryptographically signed in a manner that facilitates the cryptographic authentication of those files by the payment terminal in accordance with B.2.8.	**Identify** any documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in any documentation, evidence, and software test results that confirms that all prompt files are cryptographically signed in a manner that supports the cryptographic authentication of those files by an underlying payment terminal in accordance with B.2.8.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective B.3: Terminal Software Attack Mitigation Software security controls are implemented to mitigate software attacks.					
B.3.1 The software validates all use 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** ☐	**N/A** ☐	**Not in Place** ☐
B.3.1.a The assessor shall examine all relevant software documentation and source code necessary to identify all external inputs to the software. For each user or other external input, the assessor shall examine all relevant software documentation and source code to confirm that inputs conform to a list of expected characteristics and that all input that does not conform to expected characteristics is rejected by the software or otherwise handled securely.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that all software inputs are checked upon data entry to determine whether the data conforms to a set of expected characteristics.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that all input data that does not conform to the set of expected characteristics are either rejected or handled in a secure manner.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
B.3.1.b The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.) 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the software testing results that confirms that all software inputs are validated upon data entry.				
	Describe what the assessor observed in the software testing results that confirms all invalid data or data that does not conform to expected characteristics are either rejected or handled securely.				
B.3.1.1 All string values are validated by the software.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.3.1.1.a The assessor shall examine all relevant software documentation and source code necessary to identify all terminal software functions where string values are passed as inputs to confirm that all strings are checked for text or data that can be erroneously or maliciously interpreted as a command.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which source code was examined in support of this test requirement.				
	Describe how the assessor ensured that all software inputs where input data is passed to the software as a string value were identified and checked for compliance with the parent control objective.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that all input data that passes to the software as a string value is checked for text or data that may be erroneously or maliciously interpreted as a command.		
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that all such values are either rejected or handled securely.		
	Where the software handles such input data rather than rejecting it, **describe** each of the methods implemented by the software to ensure such input data is handled safely.		
B.3.1.1.b The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.), 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the software testing results that confirms that all input data containing commands is either rejected or handled safely and securely.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
B.3.1.2.a The assessor shall examine all relevant software documentation and source code necessary to identify all software functions that handle buffers and process data supplied by external inputs. 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 that 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which source code was examined in support of this test requirement.				
	Describe how the assessor ensured that all software inputs that handle buffers and process externally provided data were identified.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that only unsigned variables are used to define buffer sizes.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that the software conducts checks to confirm that buffers are sized appropriately wherever the software handles buffers.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that all input data that violates buffer size or other memory allocation thresholds are rejected or handled securely.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Where the software handles input data that violates buffer size or other memory thresholds rather than rejecting it, **describe** the methods implemented by the software to ensure such input data is handled securely.				
B.3.1.2.b The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.) 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the software testing results that confirms that all input data that violates buffer size or other memory allocation thresholds is rejected or handled securely.				
B.3.2 Return values are checked, and error conditions are handled securely.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.3.2.a The assessor shall examine all relevant software documentation and source code necessary to identify all software functions that handle the sensitive data predefined in Control Objective 1.2. 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms that the software performs checks on return values to ensure that sensitive data is not inadvertently leaked through error codes or messages.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
B.3.2.b The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.), 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	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.				
	Describe what the assessor observed in the software testing results that confirms that sensitive data is not exposed or inadvertently leaked through error codes or messages.				
B.3.3 Race conditions are avoided.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.3.3.a The assessor shall examine all relevant software documentation and source code necessary 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe how and the extent to which source code was examined in support of this test requirement.				
	Describe what the assessor observed in the documentation, evidence, and source code that confirms protection mechanisms are implemented in the software to mitigate race conditions.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
B.3.3.b The assessor shall install and configure the software in accordance with the software vendor's implementation guidance required in Control Objectives 12.1 and B.5.1. Using an appropriate "test platform" and suitable forensic tools and/or methods (commercial tools, scripts, etc.), 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	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.		
	Describe what the assessor observed in the software testing results that confirms that the software is resistant to race conditions.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
Control Objective B.4: Terminal Software Security Testing The software is tested rigorously for vulnerabilities prior to each release.					
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** ☐	**N/A** ☐	**Not in Place** ☐
B.4.1.a The assessor shall examine all relevant software documentation and evidence necessary 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Summarize the software vendor's process for testing the software for vulnerabilities or other software flaws prior to software release.				
	Describe when and the frequency with which the software is tested for the presence or use of any unnecessary ports and protocols prior to software release.				
	Describe when and the frequency with which the software is tested for the unintended storage, transmission, or output of clear-text account data.				
	Describe when and the frequency with which the software is tested for the presence of any default user accounts with default or static access credentials.				
	Describe when and the frequency with which the software is tested for the presence of any hard-coded authentication credentials in code or in configuration files.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe when and the frequency with which the software is tested for the presence of any test data or test accounts.		
	Describe when and the frequency with which the software is tested for the presence of any faulty or ineffective software security controls.		
B.4.1.b The assessor shall examine all relevant documentation and evidence necessary (such as software testing artifacts, etc.) 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 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.	**Identify** the documentation and evidence examined in support of this test requirement.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software is routinely tested for the presence or use of unnecessary ports or protocols.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software is routinely tested for the unintended storage, transmission, or output of clear-text account data.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software is routinely tested for the presence of default user accounts with default or static access credentials.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software is routinely tested for the presence of hard-coded authentication credentials in code or in configuration files.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	Describe what the assessor observed in the documentation and evidence that confirms that the software is routinely tested for the presence of test data or test accounts.		
	Describe what the assessor observed in the documentation and evidence that confirms that the software is routinely tested for the presence of faulty or ineffective software security controls.		

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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.					
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** ☐	**N/A** ☐	**Not in Place** ☐
B.5.1 The assessor shall examine all relevant software documentation and evidence necessary to confirm that the software vendor provides detailed implementation guidance to stakeholders in accordance with Control Objective 12.1 on how to securely implement and operate the software for all applicable payment terminals.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor provides detailed guidance to stakeholders on how to securely implement and operate the software for all payment terminals on which the software is to be deployed.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor's guidance is provided to stakeholders in accordance with Control Objective 12.				
B.5.1.1 Implementation guidance includes detailed instructions for how to configure all available security options and parameters of the software.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.5.1.1 The assessor shall examine software vendor implementation guidance to confirm it includes detailed instructions on how to configure all available security options and parameters of the software in accordance with Control Objective B.1.3.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that indicates that the software vendor's guidance covers all available software security options and parameters.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
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** ☐	**N/A** ☐	**Not in Place** ☐
B.5.1.2 The assessor shall examine the software vendor implementation guidance to confirm it includes detailed instructions on how to securely configure the software to use the security features and functions of the payment terminal where applicable.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that indicates that the software vendor's guidance covers all payment terminal security features and functions used by the software.				
	Describe what the assessor observed in the documentation and evidence that demonstrates that the software vendor's guidance covers the secure configuration and use of security features and functions for all payment terminals upon which the software is to be deployed.				
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** ☐	**N/A** ☐	**Not in Place** ☐
B.5.1.3 The assessor shall examine the software vendor implementation guidance to confirm it 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.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that indicates that the software vendor's guidance covers all payment terminal shared resources used by the software.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	Describe what the assessor observed in the documentation and evidence that demonstrates that the software vendor's guidance covers the secure integration and use of shared resources for all payment terminals upon which the software is to be deployed.				
B.5.1.4 Implementation guidance includes detailed instructions on how to cryptographically sign the software files in a manner that facilitates the cryptographic authentication of all such files by the payment terminal.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.5.1.4 The assessor shall examine the software vendor implementation guidance to confirm it includes detailed instructions on how to cryptographically sign the software files in a manner that facilitates the cryptographic authentication of all such files by the payment terminal in accordance with Control Objective B.2.8.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that indicates that the software vendor's guidance covers cryptographic signing for all software files.				
	Describe what the assessor observed in the documentation and evidence that demonstrates that the software vendor's guidance covers cryptographic signing for all payment terminals upon which the software is to be deployed.				
B.5.1.5 Implementation guidance includes instructions for stakeholders to cryptographically sign all prompt files.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.5.1.5 The assessor shall examine the software vendor implementation guidance to confirm it includes detailed instructions for stakeholders to cryptographically sign all prompt files in accordance with Control Objective B.2.9.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that confirms that the software vendor's guidance covers cryptographic signing of all prompt files.				

Control Objective and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
B.5.2 Implementation guidance adheres to payment terminal vendor guidance on the secure configuration of the payment terminal.			**In Place** ☐	**N/A** ☐	**Not in Place** ☐
B.5.2 The assessor shall examine the payment terminal vendor's security guidance/policy and the software implementation guidance required in Control Objective B.5.1 to confirm that the software implementation guidance aligns with the payment terminal vendor's security guidance/policy.	**Identify** the documentation and evidence examined in support of this test requirement.				
	Describe what the assessor observed in the documentation and evidence that demonstrates the software vendor's guidance for securely configuring the underlying payment terminal aligns with the payment terminal vendor's security guidance for each payment terminal upon which the software is to be deployed.				

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 Reporting Details column for that test requirement that additional information is recorded in Appendix A.

Control Objective	Test Requirement	Additional Information
Example:		
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 4.5.1 of the *Secure Software Program Guide*. This confirmation must be submitted to PCI SSC with the completed *Report on Validation (ROV)*.

B.1 Confirmation of Testing Environment Used	
The Secure Software Assessor Company's Testing Environment, as describe in Section 4.5.1 of the *Secure Software Program Guide*, was used for this assessment. ***Note**: 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.2 Confirmation of Testing Environment Configuration	
For each of the unique combinations of testing hardware, software and system configurations specified in Section 3.4, confirm the following: ***Note**: If any of the questions below are determined to be "not applicable," please select "No" for the response and provide a detailed explanation as to why the questions are not applicable in B.3 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

B.2 Confirmation of Testing Environment Configuration (continued)	
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.3 Attestation of Test Environment Validation	
Provide the name of the Secure Software Assessor who attests that all items in table B.1 and B.2 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.2 were marked as "No," please 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.	