Payment Card Industry

# Software Security Framework

## Template for Report on Validation

### For use with PCI Secure Software Standard v1.0

**Revision 1.0**

September 2019

# Document Changes

| Date | Version | Description |
|---|---|---|
| September 2019 | Revision 1.0 | Initial release of the Report on Validation (ROV) template for the PCI Secure Software Standard v1.0. |

# Table of Contents

# Introduction to the PCI Secure Software Report on Validation Reporting Template

This document, the PCI Software Security Framework – Secure Software Report on Validation Reporting Template (which will subsequently be 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") 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 to use. Using this template assures a consistent level of reporting against the PCI Secure Software Standard amongst assessors.

**Note: Use of this Reporting Template is mandatory for all Secure Software Assessment report submissions to PCI SSC.**

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase or decrease the number of rows or to change column width. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed by the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos, is acceptable 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 the report is written and for the recipient in understanding the context the responses and conclusions are made. Additional text or sections is permitted within reason, as noted before.**

A Secure Software Assessment involves thorough testing and assessment activities, from which the assessor will generate 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 provides 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.

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

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

## 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:

A. Additional Information Worksheet

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** 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 or individuals interviewed demonstrate a control objective was met, or how the assessor concluded an implemented security control is fit-for-purpose.<br>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 vendor 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, 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".<br>***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 particular 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.<br>• Read and understand the intent of each control objective and test requirement.<br>• Provide a response for every reporting instruction.<br>• Provide sufficient detail and information to demonstrate a finding of "In Place" or "N/A".<br>• Describe how a control objective was verified as the reporting instruction directs, not just that it was verified.<br>• Ensure that all parts of the test requirements and reporting instructions are addressed.<br>• Ensure the response covers all applicable systems, processes, and components including those provided by third-parties.<br>• Perform an internal quality assurance review of the ROV for clarity, accuracy, and quality.<br>• Provide useful, meaningful diagrams, as directed.<br>• 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".<br>• Do not include forward-looking statements or project plans in the "In Place" column.<br>• Do not simply repeat or echo the test requirements in the response.<br>• Do not copy responses from one test requirement to another.<br>• Do not copy responses from previous assessments.<br>• 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 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 3.7.

## 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 5.5.1 of the *Secure Software Standard 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<br>*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:<br>***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:<br>***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: | |
| Product category for this software (Please refer to Section A.3 of the Secure Software Standard Program Guide for a detailed explanation of product categories): | | | |
| ☐ (01) POS Suite/General<br>☐ (02) Payment Middleware<br>☐ (03) Payment Gateway/Switch | ☐ (04) Payment Back Office<br>☐ (05) POS Admin<br>☐ (06) POS Specialized | ☐ (07) POS Kiosk<br>☐ (08) POS Face-to-Face/POI<br>☐ (09) Shopping Cart / Store Front | ☐ (10) Card-Not-Present<br>☐ (11) Automated Fuel Dispenser<br>☐ (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, other systems or components it typically interacts with, etc.) | | | |
| | | | |

| 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):<br>***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 are defined.*

| ***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*** *(Microsoft Active Directory, OpenSSL, iOS, 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 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:<br><br>***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<br>☐ Module A – Account Data Protection |

| 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 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 Sample Sets Used

Identify and list all of 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 |
|---|---|---|---|---|
| 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 scepticism;
- This Report on Validation accurately identifies, describes, represents and characterizes all of 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 Standard 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 3.6: 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

## Security Objective: 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 functionality 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**<br>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), as well as 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 vendor evidence examined that details all of the sensitive data that is stored, processed and/or transmitted by the software in accordance with this test requirement. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 Test Requirement 1.1.a, **identify** the vendor 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. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude it details all locations where sensitive data is stored, including 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). | | |
| **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 vendor evidence examined that describes where the implementation enforces storage within a specific location or form factor. | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of the software tests are supported by the vendor evidence. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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.<br><br>***Note:*** *The assessor may require and rely on assistance from the vendor to fulfill this test requirement (such as through access to a dedicated test environment). Any such specific assistance must be documented by the assessor.* | **Describe** each of the software tests performed to identify all sensitive data that is stored, processed, and/or transmitted by the software (to validate the information obtained in Test Requirement in 1.1.a). | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of the testing are supported by the vendor evidence obtained in Test Requirement 1.1.a. | | |
| **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 vendor evidence examined that identifies the transaction types and/or card data elements that are supported by the software. | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of the testing are supported by the vendor evidence. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 vendor evidence examined that describes all cryptographic implementations supported by the software, including (but not limited to) cryptography used for storage, transport, and authentication, and whether the cryptography is implemented by the software itself, through third-party software, or as functions of the execution environment. | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of the testing are supported by the vendor evidence. | | |
| **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 vendor evidence examined that identifies all accounts or authentication credentials supported by the software, including both default and user created accounts. | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of the testing are supported by the vendor evidence. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 vendor evidence examined that outlines all configuration options provided by the software that can impact sensitive data. | | |
| | **Describe** the criteria the assessor used to determine whether configuration options provided by the software have the potential to impact sensitive data. | | |
| | **Describe** each of the software tests performed to validate the configuration options specified in the vendor evidence. | | |
| **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. | **Indicate** whether the software uses cryptography to protect any sensitive data (yes/no). | | |
| | *If "yes,"* **identify** the vendor evidence examined that describes all cryptographic methods and materials used to protect sensitive data. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) | | |
|---|---|---|---|---|---|
| **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 vendor evidence examined that details all the sensitive functions and sensitive resources provided or used by the software. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that it covers all functions that are designed to store, process and transmit sensitive data. | | | | |
| **1.2.b** For each of the sensitive functions listed, the assessor shall examine vendor evidence to confirm that vendor evidence clearly describes how and where the sensitive data associated with this function 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 vendor evidence examined that describes how and where sensitive data associated with each sensitive function is stored, including in temporary storage, semi-permanent storage, and non-volatile storage. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **1.2.c** Where the sensitive functions 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.<br>***Note:*** *For example, by reviewing the security policy of a PTS or FIPS140-2 approved cryptographic system.* | **Identify** the vendor evidence examined that describes whether any sensitive functions are provided by third-party software or systems. | | |
| | **Indicate** whether the software relies upon sensitive functions provided by third-party software or systems (yes/no).<br>*If "no," skip to 1.2.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the available implementation guidance examined for third-party software or systems providing sensitive functions to the vendor software. | | |
| | **Describe** each of the software tests performed to determine whether the vendor software is correctly following the implementation guidance for each instance where the software relies on sensitive functions provided by third-party software or systems. | | |
| | **Describe** what the assessor observed through testing to conclude the that vendor software is correctly following all available third-party implementation guidance. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of the testing are supported by the vendor evidence examined in Test Requirement 1.2.a. | | |

| 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:<br>• The vendor defines classification criteria for identifying critical assets;<br>• Vendor classification criteria identifies the confidentiality, integrity, and resiliency requirements for each critical asset; and<br>• An inventory of all critical assets with appropriate classifications is defined. | **Identify** the vendor evidence examined that confirms the vendor identifies and classifies critical assets. | | | | |
| | **Summarize** the vendor's classification criteria and how it classifies critical assets. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that an inventory of all critical assets with appropriate classifications is defined and maintained. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) | | |
|---|---|---|---|---|---|
| **Control Objective 2: Secure Defaults**<br>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 install. 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).<br>***Note:*** *This includes functions which are auto-enabled as required during operation of the software.* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Describe** each of the tests performed to validate the software APIs and other interfaces specified in the vendor evidence, including those tests intended to reveal any exposed functionality of the software (such as scanning for listening services). | | | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of the testing are supported by the vendor evidence. | | | | |
| **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 as required in Control Objective 5. 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.<br>*(continued on next page)* | **Describe** each of the software tests performed to determine whether any of the functions identified in Test Requirement 2.1.a rely on external resources for authentication. | | | | |
| | **Indicate** whether the software relies upon such external resources for authentication for APIs or other interfaces (yes/no).<br>*If "no," skip to 2.1.c.*<br>*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) |
|---|---|---|---|
| | For each instance where the software relies upon external resources for API authentication, **identify** the external resources used. | | |
| | **Identify** the vendor evidence examined that details 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 by default. | | |
| **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 as required in Control Objective 6. 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. | **Describe** each test performed 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. | | |
| | **Indicate** whether such external resources are relied upon for the protection of sensitive data during transmission (yes/no).<br>*If "no," skip to 2.1.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | For each instance where the software relies upon external resources for the protection of sensitive data during transmission, **identify** the external resources used. | | |
| | **Identify** the vendor evidence examined that details all methods required to ensure proper protection of sensitive data remains in place in accordance with Control Objective 6. | | |

| 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** the public vulnerability repositories that were searched to determine whether any of the functions identified in Test Requirement 2.1.a expose methods or services which have publicly disclosed vulnerabilities. | | |
| | **Describe** each of the software tests performed to confirm whether any of the functions identified in Test Requirement 2.1.a expose methods or services that are vulnerable to attacks. | | |
| **2.1.e** Where vulnerabilities in exposed functions exist, the assessor shall examine vendor evidence and test the software to confirm the following:<br>• The mitigations implemented by the software vendor to minimize exploit of these weakness have been identified.<br>• The risks posed by the use of known vulnerable protocols, functions, or ports is documented.<br>• 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.<br><br>*(continued on next page)* | **Indicate** whether any of the functions identified Test Requirement 2.1.a expose methods or services which have publicly disclosed vulnerabilities (yes/no).<br>*If "no," skip to 2.1.f.*<br>*If yes," complete the reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that confirms the risks posed by the use the vulnerable functions, protocols, ports, etc are known and documented. | | |
| | **Identify** the vendor evidence examined that details the mitigations implemented by the software vendor to minimize exploit of the vulnerabilities. | | |
| | **Describe** each of the software tests performed to confirm that the vulnerabilities have been mitigated in accordance with vendor documentation. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| ***Note:*** *The assessor should reference the vendor threat model as defined under Control Objective 4 for this item.* | **Identify** the vendor evidence examined that confirms the vendor has made guidance available to stakeholders (in accordance with Control Objective 12) on how to correctly implement the mitigations required to minimize the exploit of the vulnerabilities. | | |
| | **identify** the page(s) or section(s) within the vendor guidance where the implementation of mitigations required to minimize the exploit of vulnerabilities is covered. | | |
| **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). | **Describe** any additional testing performed (in addition to the testing performed in Test Requirement 2.1.a) to identify all functions exposed by the software. | | |
| | **Describe** what the assessor discovered through additional testing to conclude that the results of the testing are supported by the vendor documentation. | | |

| 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 either disabled, unable to be accessed through mitigation methods implemented by the software, or is formally documented and justified by the vendor.<br><br>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.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | |
| | **Indicate** whether third-party modules (i.e., functions, libraries, etc.) are used by the software (yes/no).<br><br>*If "no," skip to 2.2.*<br><br>*If "yes," complete the remining reporting instructions for this test requirement.*<br><br>***Note**: The response to this reporting instruction should be consistent with the software components identified in Section 2.5.* | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that all functionality exposed by each third-party module is either disabled, unable to be accessed, or is formally documented and justified by the software vendor. | | |
| | **Indicate** whether access to third-party modules/functions is prevented through mitigation methods (yes/no).<br><br>*If "no," skip to 2.2.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed to determine whether mitigation methods rely on a lack of knowledge of the modules/functions as their mitigation method. | | |

| 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 testing results to conclude that the implemented mitigations are effective at preventing the insecure use of such third-party modules/functions. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) | | |
|---|---|---|---|---|---|
| **2.2 All software security controls, features, and functionalities 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 features and to confirm that any security features relied upon by the software for the protection of critical assets are enabled upon installation, initialization, or first use of the software. | **Identify** the vendor evidence examined that identifies all software security controls, features and functionalities implemented or provided by the software. | | | | |
| | **Describe** each of the software tests performed in support of this test procedure. | | | | |
| | **Describe** what the assessor observed in the vendor evidence and through testing to conclude that all software security features relied upon for the protection of critical assets are enabled upon software installation, initialization, or first use. | | | | |
| **2.2.b** Where any security features 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. | **Identify** the vendor evidence examined that details any security controls, features or functionalities enabled by default. | | | | |
| | **Indicate** whether security controls, features, and functionalities relied upon for the protection of critical assets are enabled only upon initialization or first use – i.e., not upon installation (yes/no). | | | | |
| | *If "yes,"* **summarize** how the software prevents sensitive data from being processed until the initialization process is complete. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **2.2.c** Where user input or interaction is required to enable any security features (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 vendor security guidance documents made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that details the security features that require user input or interaction to be enabled. | | |
| | **Indicate** whether any security controls, features, and functionalities relied upon for the protection of critical assets require user input or interaction to be enabled (yes/no).<br>*If "no," skip to 2.2.d.*<br>If "yes," complete the remining reporting instructions for this test requirement. | | |
| | **Identify** the vendor security guidance examined, and the page(s) or section(s) within the guidance where the process to enable such features is covered. | | |
| | **Describe** what the assessor observed in the vendor guidance to conclude the instructions provided in the guidance for stakeholders are appropriate for properly enabling the security controls, features, and functionalities. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **2.2.d** The assessor shall examine vendor evidence and test the software to confirm that through following the provided vendor security guidance (per Control Objective 12), all security-relevant features, controls, and functionalities are enabled prior to the software enabling processing of sensitive data. | **Describe** each of the tests performed to determine whether following the vendor's security guidance results in all security-relevant features, controls, and functionalities enabled prior to the software enabling processing of sensitive data. | | |
| | **Describe** what the assessor observed in the vendor security guidance and through testing to conclude that following the vendor's security guidance results in all security-relevant features, controls, and functionalities enabled prior to the software enabling processing of sensitive data. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) | | |
|---|---|---|---|---|---|
| **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.<br><br>***Note:*** *The assessor should refer to Control Objectives 1, 5, and 7 to identify authentication and access control mechanisms, keys, and other critical assets used for authentication.* | **Identify** the vendor evidence examined that details all default credentials, keys, certificates, and other critical assets used for authentication by the software. | | | | |
| **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.<br><br>***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 tests performed to validate the default credentials, keys, certificates and other critical assets specified in the vendor evidence. | | | | |
| | **Describe** what the assessor observed through testing to conclude the results of the testing are supported by the vendor evidence examined in Test Requirement 2.3.a. | | | | |

| 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 vendor security guidance documents made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that details all instances where user input or interaction is required to disable or change any authentication credentials or keys for built-in accounts. | | |
| | **Indicate** whether user input or interaction is required to disable or change any authentication credentials or keys for built-in accounts (yes/no).<br>*If "no," skip to 2.3.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor security guidance examined, and the page(s) or section(s) within the guidance where the process to disable or change such authentication credentials or keys is covered. | | |
| **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 mechanisms implemented by the software.<br>***Note:*** *The assessor should refer to Control Objective 5 to identify authentication and access mechanisms.* | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the testing results that provide reasonable assurance that built-in accounts are not used by the authentication and access mechanisms implemented by the software. | | |

| 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.<br><br>***Note:*** *The assessor should refer to Control Objective 6 to identify security control used to protect sensitive data.* | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the testing results that provide reasonable assurance that default authentication credentials or keys for built-in accounts are not used to protect the storage and transmission of sensitive data. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) | | |
|---|---|---|---|---|---|
| **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 vendor evidence examined that details all privileges and resources required by the software, and the vendor's justifications for their use. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the vendor's justifications for all 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 vendor security guidance documents made available to stakeholders per Control Objective 12.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that describes whether any limitations exist within the architecture of the software or its intended execution environment that would otherwise preclude restricting the software's privileges or ability access to resources within the intended execution environment. | | | | |
| | **Indicate** whether any such limitations were found to exist (yes/no).<br><br>*If "no," skip to 2.4.c.*<br><br>*If "yes," complete the remaining reporting instructions for this Test Requirement.* | | | | |
| | For each instance where such limitations exist**, summarize** the limitations that prevent restricting the software's privileges or ability to access resources within the intended execution environment. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| | **Identify** the vendor evidence that details the mechanisms implemented by the software to prevent unauthorized access, exposure, or modification of critical assets. | | |
| | **Identify** the vendor security guidance examined, and the page(s) or section(s) within that guidance where the proper implementation of such mechanisms is covered. | | |
| **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.<br><br>***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 tests performed to validate the privileges and access permissions detailed in the vendor evidence. | | |
| | **Identify** the tools used by the assessor to validate the privileges and access permissions. | | |
| | Where the use of suitable tools is not possible, **describe** the assessor's rationale for concluding that the testing performed is sufficient. | | |

| 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 vendor evidence examined that details whether the software execution environment provides any legacy features. | | |
| | **Indicate** whether the intended software execution environment provides such legacy features (yes/no).<br>*If "no," skip to 2.5.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the tests performed to determine whether the software uses any of the legacy features provided by the software execution environment. | | |
| | **Describe** what the assessor observed in vendor evidence and discovered through testing to conclude that such legacy features are not used, and that only recent and secured functionality is implemented. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) | | |
|---|---|---|---|---|---|
| **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 vendor evidence examined that details all the default accounts provided by the software and the privileges assigned to these accounts. | | | | |
| | **Identify** the vendor evidence examined that details all of the vendor's justifications for the privileges assigned to default accounts. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude the justifications for the privileges assigned to 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. | | | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of testing are supported by the vendor evidence. | | | | |
| **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 vendor evidence examined that details the mechanisms implemented to protect exposed functionalities (i.e., APIs) from use by authorized users in an attempt to modify account privileges and elevate user access rights. | | | | |
| *(continued on next page)* | **Describe** each of the software tests 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) |
|---|---|---|---|
| | **Describe** what the assessor observed in vendor evidence and discovered through testing to conclude that exposed functionalities (i.e., APIs) are appropriately 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**<br>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**<br>☐ | **N/A**<br>☐ | **Not in Place**<br>☐ |
| **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.<br>***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets, including retained sensitive data.* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the vendor's justifications for retaining each item of 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 sensitive data are supported by the vendor evidence.<br>***Note:*** *The assessor should refer to Control Objective 1 to identify all sensitive functions and services.* | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor discovered through testing to conclude the results of software testing are supported by the vendor evidence. | | | | |

| 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 is 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. | **Describe** the software tests performed in support of this test requirement. | | |
| | **Indicate** whether the software allows for sensitive data to be stored or retained solely for the purposes of debugging, error finding, or testing (yes/no).<br>*If "no," skip to 3.1.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** the mechanisms implemented by the software to ensure that sensitive data storage or retention for the purposes of debugging, error finding, or testing is explicitly enabled and authorized by the user. | | |
| | **Describe** each of the software tests performed to determine whether sensitive data stored or retained for the purposes of debugging, error finding, or testing is protected in accordance with Control Objective 6. | | |
| | **Describe** what the assessor discovered through testing to confirm that sensitive data stored or retained for these purposes is only for a reasonable and necessary duration in accordance with vendor's criteria for sensitive data retention. | | |
| | **Describe** the mechanisms implemented by the software to ensure that sensitive data stored or retained for these purposes is not retained upon closure of the software. | | |

| 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, including secure deletion procedures per Control Objective 3.4, provided in the vendor security guidance documents made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that details whether user input or interaction is required to configure the retention period of sensitive data. | | |
| | **Indicate** whether the retention of any sensitive data requires such user input or interaction to configure the retention period (yes/no).<br>*If "no," skip to 3.2.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** what the assessor observed in the vendor security guidance to conclude it provides clear and sufficient instruction for stakeholders on the proper configuration of retention periods and secure deletion procedures. | | |
| | **Identify** the page(s) or section(s) in the vendor security guidance where configuration of retention periods and secure deletion procedures is covered. | | |

| 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.<br>***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets, including transient sensitive data.* | **Identify** the vendor evidence examined that details all sensitive data that is retained by the software for transient use. | | | | |
| | **Identify** the vendor evidence examined that includes all justifications for retaining such data. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude the vendor's justifications for retaining sensitive data for transient use, including sensitive data stored in memory during operation of the software, 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.<br>***Note:*** *The assessor should refer to Control Objective 1 to identify all sensitive functions and services.* | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor observed in the testing results that provides reasonable assurance that the software does not use immutable objects. | | | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of the testing are supported by the vendor evidence. | | | | |

| 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 sensitive data stored solely for the purposes of debugging, error finding, or testing of systems is protected in accordance with Control Objective 6. Where data is stored for the sole purpose of debugging, error finding, or testing of systems, the assessor shall confirm that the functionality that allows for storage of 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 sensitive data is securely deleted per Control Objective 3.4. | ***Note**: This test requirement is a duplicate of 3.1.c. Reporting instructions are intentionally left blank. No further instruction needed.* | | |
| **3.2.d** Where users can configure retention of transient sensitive data, the assessor shall examine vendor evidence to confirm that there is clear and sufficient guidance on this process, including triggering secure deletion procedure per Control Objective 3.4, is provided in the vendor security guidance documents made available to stakeholders per Control Objective 12.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that details whether users can configure the retention of transient sensitive data. | | |
| | **Indicate** whether the retention of transient sensitive data can be configured by users (yes/no).<br><br>*If "no," skip to 3.3.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** what the assessor observed in the vendor security guidance to conclude it provides clear and sufficient instruction for stakeholders on properly configuring the retention period for transient sensitive data and triggering 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) |
|---|---|---|---|
| | **Identify** the page(s) or section(s) in the vendor security guidance where configuration of retention periods for transient sensitive data and triggering secure deletion of such data when no longer needed is covered. | | |

| 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.<br>***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets.* | **Identify** the vendor evidence examined that details the protection methods implemented for all sensitive data during storage and transmission. | | | | |
| **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 to confirm that there is no additional storage of sensitive data other than that which was covered in 3.3.a. | | | | |
| | **Describe** how the results of testing provide reasonable assurance that no additional storage of sensitive data is included beyond those methods identified in 3.3.a. | | | | |
| **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 vendor evidence examined that details whether sensitive data is stored outside of temporary variables within the software code. | | | | |
| | **Indicate** whether such instances of sensitive data storage were found (yes/no).<br>*If "no," skip to 3.3.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | | | |
| *(continued on next page)* | **Describe** each of the software tests 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) |
|---|---|---|---|
| | **Describe** what the assessor observed in the testing results to conclude that all instances of sensitive data stored outside of temporary variables within the software code are protected using either strong cryptography or with other methods that provide an equivalent level of security. | | |
| **3.3.d** Where protection methods use cryptography, the assessor shall examine vendor evidence and test the software to confirm that the method complies with Control Objective 7 of this standard. | **Identify** the vendor evidence examined that details all sensitive data protection methods that use cryptography. | | |
| | **Indicate** whether cryptography is used to protect sensitive data stored or retained by the software (yes/no). | | |
| | *If "yes,"* **describe** what the assessor observed in the vendor evidence and discovered through testing to conclude that cryptographic methods used for protecting the sensitive data comply 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.<br><br>*(continued on next page)* | **Identify** all vendor evidence examined that details whether any sensitive data is protected using methods other than strong cryptography. | | |
| | **Indicate** whether such methods are used to protect sensitive data during storage or retention (yes/no).<br>*If "no," skip to 3.3.f.*<br>*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) |
|---|---|---|---|
| | **Identify** the vendor evidence examined that details the protections provided for each environment in which the software is designed to be executed. | | |
| | **Describe** each of the software tests performed to confirm that the protections are present in all environments where the software is designed to be executed and are correctly implemented. | | |
| | **Describe** what the assessor discovered through testing to conclude the results of software testing are supported by the vendor evidence. | | |
| **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 vendor security guidance documents made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that details whether any protection mechanisms implemented to safeguard sensitive data require user configuration to be enabled. | | |
| | **Indicate** whether the software requires user interaction to configure the protection methods identified in 3.3.a, 3.3.d and 3.3.e (yes/no).<br>*If "no," skip to 3.4.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| *(continued on next page)* | **Describe** what the assessor observed in the vendor security guidance to conclude it provides clear and sufficient instruction for stakeholders on the proper configuration of such protection mechanisms. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| | **Identify** the page(s) or section(s) in the vendor security guidance where configuration of such protection mechanisms is covered. | | |

| 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 outlined in Control Objective 3.1. | **Identify** the vendor evidence examined that details all methods implemented by the software to securely delete non-transient sensitive data when no longer required. | | | | |
| | **Summarize** the methods implemented by the software to securely delete non-transient sensitive data when no longer needed. | | | | |
| **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 such 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-leveling algorithms or SSD over-provisioning, which may complicate simple over-writing methods. | **Identify** the vendor evidence examined that details whether any platform or implementation-level issues complicate secure deletion of transient sensitive data. | | | | |
| | **Indicate** whether any such issues exist (yes/no).<br>*If "no," skip to 3.4.c.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that each of the secure deletion methods implemented by the software successfully render the applicable sensitive data unrecoverable. | | | | |
| | **Describe** how such methods accommodate for platform-specific issues, such as flash wear-leveling 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, including usage of forensic tools, to identify any 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 as defined in Control Objective 3.1.<br><br>***Note:*** *Where forensic testing of the 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, including the details of the forensic tools used, to determine whether sensitive data residue is persistent in the execution environment after execution of the secure deletion methods described in 3.4.a. | | |
| | **Describe** how each of the software tests performed accommodates for the data structures and methods used to store non-transient sensitive data. | | |
| | **Describe** what the assessor observed in vendor evidence and the test results that conclude that the secure deletion methods identified in 3.4.a are implemented correctly and are applied to all non-transient sensitive data. | | |

| 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 outlined in Control Objective 3.2, and to confirm that these methods ensure that the data is unrecoverable after deletion.<br><br>***Note:*** *This includes data which may be stored only temporarily in program memory / variables during operation of the software.* | **Identify** the vendor evidence examined that details all methods implemented by the software to securely delete the transient sensitive data once the purpose for which it is retained is satisfied. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the secure deletion methods implemented by the software are sufficient to render transient sensitive data unrecoverable after deletion. | | | | |
| **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 vendor evidence examined that details whether any platform or implementation-level issues exist that complicate the erasure of transient sensitive data. | | | | |
| | **Indicate** whether such issues were found to exist (yes/no).<br><br>If "no," skip to 3.5.c.<br><br>If "yes," complete the remaining reporting instructions for this test requirement. | | | | |
| | **Summarize** the methods implemented by the software to compensate for such platform or implementation issues. | | | | |
| | **Describe** what the assessor observed in the vendor evidence and discovered through testing to conclude the methods implemented are sufficient to minimize the risk posed by such platform or implementation issues. | | | | |

| 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 as defined in Control Objective 3.1.<br><br>***Note:*** *Where forensic testing of the 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, including the details of the forensic tools used, to determine whether transient sensitive data residue is persistent in the execution environment after execution of the secure deletion methods described in 3.5.a. | | |
| | **Describe** how each of the software tests performed accommodate for the data structures and methods used to store transient sensitive data. | | |
| | **Describe** what the assessor observed in vendor evidence and the test results that confirm the secure deletion methods identified in 3.5.a are implemented correctly and are 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 that software vendor has performed a thorough analysis to account for all sensitive data disclosure attack vectors including, but not limited to:<br>• Error messages, error logs, or memory dumps.<br>• 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.<br>• 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.<br>• 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 vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the software vendor's analysis accounted for each of the attack vectors described in this test requirement. | | | | |
| | **Identify** any additional sensitive data disclosure attack vectors covered in the vendor's analysis. | | | | |

| 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 3.2.a, and test the software to confirm the software vendor implemented mitigations to protect from 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 vendor evidence examined that details all of the mitigations implemented by the software to protect sensitive data from disclosure through unintended channels. | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that protection mechanisms are properly implemented to protect against the unintended disclosure of sensitive data in accordance with the vendor evidence. | | |
| **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 vendor security guidance documents made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | |
| | **Identify** the page(s) or section(s) within the vendor guidance that covers the proper configuration and use of the protection mechanisms identified in 3.6.b. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **3.6.d** The assessor shall test the software, including usage of forensic tools, to identify any sensitive data residue in the execution environment and forcing errors, such as through user and network interfaces, to confirm that all mitigation controls are implemented correctly and that the software does not expose or otherwise reveal sensitive data. | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the testing results to conclude that all mitigation controls to protect against the exposure of sensitive data are implemented correctly. | | |
| | **Describe** what the assessor observed in the test results that provides reasonable assurance the software does not expose or otherwise reveal sensitive data. | | |

## Security Objective: 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**<br>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 vendor evidence examined that details all of the attack scenarios relevant to the software, and the protection mechanism implemented to mitigate the 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 vendor evidence examined that details the vendor's methodology for determining attack scenarios relevant to the vendor's software. | | | | |
| | **Indicate** whether industry-standard methods are used as the basis for the vendor's methodology (yes/no). | | | | |
| | *If "yes,"* **identify** the industry-standard methods or guidelines used. | | | | |
| | *If "no,"* **describe** how the vendor's methodology provides equivalent methods as industry-standard methods and provides equivalent coverage of the attack scenarios applicable to the assessed software. | | | | |

| 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:<br>• A formal owner of the software application 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.<br>• A methodology is defined for measuring the likelihood and impact for any exploit of the system.<br>• Generic threat methods and types that may be applicable to the software are documented.<br>• All critical assets managed by and sensitive resources used by the system are documented.<br>• All entry and egress methods for sensitive data by the software application, as well as the authentication and trust model applied to each of these entry/egress points, are defined.<br>• All data flows, network segments, and authentication/privilege boundaries are defined.<br>• All static IPs, domains, URLs, or ports required by the software for operation are documented.<br>*(continued on next page)* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | |
| | **Summarize** the vendor's methodology for defining and measuring the likelihood and impact of exploits for the assessed software. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that all entry and egress points for sensitive data as well as the authentication and trust model(s) applied to these entry and egress points were covered in the vendor's attack analysis. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that all data flows, network segments, and authentication/privilege boundaries of the software were covered in the vendor's attack analysis. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that all static IPs, domains, URLs, or ports required by the software for operation were covered in the vendor's attack analysis. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that cryptography and cryptographic elements, such as cipher modes, were 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) |
|---|---|---|---|
| • 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.<br>• Execution environment implementation specifics or assumptions such as network configurations, operating system security configurations, etc. are documented.<br>• Consideration for the installed environment of the software application, 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 vendor evidence to conclude that the software execution environment was considered in the vendor's attack analysis. | | |
| **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 vendor evidence examined that confirms the findings for this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the potential risks uniquely applicable to a production deployment of the assessed software were 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 attack.** | | | **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 vendor evidence examined that details all of the mitigation methods implemented to address all of the threats identified in Control Objective 4.1. | | | | |
| | **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 vendor evidence to conclude that vendor's justification(s) for any lack of mitigations 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 tests performed to determine whether the mitigation methods identified in 4.2.a are properly implemented by the software. | | | | |
| | **Describe** what the assessor observed in the vendor evidence and discovered through testing to conclude 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 install of the software. | **Identify** the vendor evidence examined that details whether any of the mitigations identified in 4.2.a rely on settings within the software and whether such settings and mitigations can be disabled, removed or bypassed by user input or interactions. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 install of the software.<br><br>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 vendor security guidance documents made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that details whether any of the mitigations identified in 4.2.a rely on settings within the software and whether such settings and mitigations can be disabled, removed or bypassed by user input or interactions. | | |
| | **Indicate** whether any of the mitigations identified in 4.2.a rely on software settings or values (yes/no).<br><br>*If "no," skip to 4.2.d.*<br><br>*If "yes," complete the remining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed to determine whether such mitigations and their associated settings are applied by default. | | |
| | **Describe** what the assessor observed in the testing results to conclude that all such settings are applied by default or that the software prevents processing of any sensitive data until such settings are applied. | | |
| | **Indicate** whether any such settings and mitigations can be disabled, removed, or bypassed by user input or interactions (yes/no).<br><br>*If "no," skip to 4.2.d.*<br><br>*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** each of the software tests performed to determine whether such action requires strong user authentication and authorization. | | |
| | **Describe** what the assessor what the assessor observed in the testing results to conclude that such actions cannot be performed without strong user authentication and authorization. | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where the risks and impacts of disabling, removing, or bypassing such mitigations are covered. | | |
| **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.<br><br>Where the execution environment provides APIs to query the status of mitigation controls, the assessor shall test the software to confirm that software checks for these mitigations are in place and active prior to being launched, and periodically throughout execution.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that details whether any mitigations rely on features of the execution environment. | | |
| | **Indicate** whether the protection mechanisms were found to rely on such features of the execution environment (yes/no).<br><br>*If "no," skip to 5.1.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where instructions on the proper enabling, configuration and usage of such features are covered. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| | **Identify** the vendor evidence examined that details whether the execution environment provides any APIs to query the status of mitigation controls. | | |
| | **Indicate** whether the execution environment provides any such APIs (yes/no).<br>*If "no," skip to Control Objective 5.*<br>*if "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed to confirm that the software checks that mitigations are in place and active during software initialization as well as throughout its execution. | | |
| | **Describe** what the assessor observed in the results of the software testing to conclude that such checks are in place and active (by default). | | |

| 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**<br>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.<br>***Note:*** *The assessor should refer to Control Objective 1 to identify asset classification and all critical assets.* | **Identify** the vendor evidence examined that details all of the authentication requirements for all roles, based on critical access classification, the type of access and the 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 vendor evidence examined that details all of the authentication implemented to control access to critical assets. | | | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor observed in the testing results to conclude that the authentication mechanisms implemented correctly in accordance with the vendor evidence. | | | | |

| 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 to the software itself, directly–the assessor shall examine vendor evidence to confirm that clear and sufficient guidance on how to configure authentication mechanisms correctly is provided in the vendor security guidance documents made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that details whether the software recommends, suggests, relies on, or otherwise facilitates the use of additional mechanisms to facilitate non-console access to the software or its underlying system. | | |
| | **Indicate** whether the software relies on or facilitates such use of additional mechanisms for secure non-console access (yes/no).<br>*If "no," skip to 5.1.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined, and the page(s) or section(s) within the guidance where instructions on the proper configuration such authentication methods are provided. | | |
| **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 vendor evidence examined that details all critical assets identified by the software vendor. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that any data associated with authentication credentials is treated as a critical asset and protected accordingly. | | |

| 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 vendor evidence examined that details all identification and authentication methods implemented by the software. | | | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the vendor observed in the vendor evidence and testing results to conclude 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 vendor security guidance documents made available to stakeholders per Control Objective 12.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that details whether interfaces, such as APIs, allow for automated access to critical access. | | | | |
| | **Indicate** whether the software provides such interfaces to enable automated access to critical assets (yes/no).<br><br>*If "no," skip to 5.2.c.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor observed in the testing results to conclude that access to the software's critical assets by different programs or systems requires unique authentication. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| | **Identify** the vendor guidance examined and the page(s) or section(s) within the guidance where instructions on configuring a unique credential for each program or system is provided. | | |
| **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.<br><br>***Note:*** *The assessor should refer to Control Objective 6 to identify controls to protect sensitive data at rest and in transit.* | **Identify** the vendor evidence examined that details whether user or system identification is supplied across a non-console interface. | | |
| | **Indicate** whether such identification is supplied (yes/no).<br><br>*If "no," skip to 5.2.d.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** the software tests performed to determine in support of this test requirement. | | |
| | **Describe** what the assessor observed in the testing results to conclude that the authentication mechanisms are appropriately protected. | | |
| **5.2.d** The assessor shall examine vendor evidence to confirm that vendor security guidance provided to stakeholders (per Control Objective 12) 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 vendor evidence examined that confirms the vendor provides security guidance on the proper use of identification and authentication parameters in accordance with Control Objective 12. | | |
| | **Identify** the page(s) or section(s) within the vendor guidance where users are instructed not to share identification and authentication parameters between individuals or programs. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 vendor evidence examined that details all methods for accessing critical assets. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that no additional methods (other than those identified in 5.2.a) are provided by the software. | | |
| | **Describe** the extent to which the source code was examined to confirm there are no other methods for accessing critical assets are provided by the software. | | |

| 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 vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that all implemented authentication methods were evaluated to identify any known vulnerabilities or attack methods for each implemented authentication method. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that all known vulnerabilities and attack methods identified are mitigated in the software implementation. | | | | |
| **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.<br><br>***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 application itself).* | **Identify** the vendor evidence examined that details the vendor's evaluation of the robustness of the authentication methods implemented by the software. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the implemented authentication methods are reasonably sufficient to protect them from being forged, spoofed, leaked, guessed or circumvented. | | | | |
| | **Describe** the methods used 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) |
|---|---|---|---|
| **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 to determine whether authentication methods are implemented correctly. | | |
| | **Describe** what the assessor observed in the testing results that provides reasonable assurance that the authentication mechanisms are correctly implemented 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 vendor evidence examined that identifies and justifies the access required for all critical assets. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the access requirements for each critical asset are reasonably justified. | | | | |
| **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** the software tests performed to identify the level of access provided to each critical asset. | | | | |
| | **Describe** what the assessor observed in the testing results to conclude that the results of the software testing are supported by the vendor evidence. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) | | |
|---|---|---|---|---|---|
| **Control Objective 6: Sensitive Data Protection**<br>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 vendor evidence examined that details all locations where sensitive data is stored by the software. | | | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor discovered through software testing to conclude that the results of the tests are supported by the vendor evidence. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that protection requirements for all sensitive data stored by the software, including requirements for rendering sensitive data with confidentiality considerations unreadable anywhere sensitive data is stored persistently, 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.<br>*(continued on next page)* | **Identify** the vendor evidence examined that details all of the security methods implemented to protect sensitive data during storage. | | | | |
| | **Describe** each of the software tests 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) |
|---|---|---|---|
| ***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.* | **Describe** what the assessor discovered through software testing to conclude the results of the tests are supported by the vendor evidence. | | |
| | **Describe** what the assessor observed in the vendor evidence and in the testing results to conclude that the security methods implemented to protect sensitive data during storage or retention appropriately address all defined protection requirements and identified attack scenarios. | | |
| **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 is compliant to Control Objective 7. | **Identify** the vendor evidence examined that details whether cryptography is used for protecting sensitive data during storage. | | |
| | **Indicate** whether cryptography is used for such purposes (yes/no).<br>*If "no," skip to 6.1.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and the testing results to conclude that all instances where cryptography is used for securing sensitive data, the cryptography is compliant 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 vendor evidence examined that details whether index tokens are used for securing sensitive data during storage. | | |
| | **Indicate** whether index tokens are used for such purposes (yes/no).<br>*If "no," skip to 6.1.e.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and the testing results to conclude that index tokens 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"). | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 vendor evidence examined that details whether protection methods rely on security properties of the execution environment. | | |
| | **Indicate** whether any protection mechanisms implemented by the software to safeguard sensitive data rely on security properties of the execution environment (yes/no).<br>*If "no," skip to 6.1.f.*<br>If "yes," complete the remaining reporting instructions for this test requirement. | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and the testing results to conclude that the security properties upon which the protection mechanisms rely exist for all platforms targeted by the software. | | |
| | **Describe** what the assessor observed in the vendor evidence and the testing results to conclude that protection mechanisms which rely on such security properties are appropriate for protecting the sensitive data. | | |

| 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 vendor evidence examined that details whether protection methods rely on security properties provided by third-party software. | | |
| | **Indicate** whether any protection mechanisms implemented by the software to safeguard sensitive data rely on the security properties of third-party software (yes/no).<br>*If "no," skip to 6.2.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and the testing results that provides reasonable assurance that there are no unmitigated vulnerabilities in the third-party software that provides the security properties the protection mechanisms rely upon. | | |

| 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 vendor evidence examined that details all locations where sensitive data is transmitted by the software. | | | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor discovered through software testing to conclude that the results of the testing are supported by the vendor evidence. | | | | |
| | **Describe** what the assessor observed in the vendor evidence examined that protection requirements are defined for all locations where sensitive data is transmitted by the software. | | | | |
| **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.<br>***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets.*<br>*(continued on next page)* | **Identify** the vendor evidence examined that details all of the ingress and egress points where sensitive data with confidentiality considerations is transmitted outside of the physical execution environment. | | | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor discovered through software testing to conclude that the results of the tests are supported by the vendor evidence. | | | | |

| 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 vendor evidence and in the testing results to conclude 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. | | |
| **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 sufficiently detailed instructions allowing for the secure settings to be applied during installation and operation of the vendor application are included in the vendor security guidance made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that details whether third-party or execution environment features are relied upon for the protection of sensitive data transmissions. | | |
| | **Indicate** whether third-party or execution-environment features are relied upon for the security of transmitted sensitive data (yes/no).<br>*If "no," skip to 6.2.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that confirms the vendor provides clear and sufficient guidance on the correct configuration and use of such third-party or execution environment features in accordance with Control Objective 12. | | |
| | **Identify** the page(s) or section(s) within the vendor guidance where the instructions on the secure configuration and use of such third-party or execution environment features are provided. | | |

| 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, assessor shall test the software to confirm that all ingress and egress methods enforce the secure version of the protocol with end-point authentication prior to the transmission of that sensitive data. | **Identify** the vendor evidence examined that details whether transport layer encryption is used to secure the transmission of sensitive data. | | |
| | **Indicate** whether transport layer encryption is used (i.e., "TLS") to secure the transmission of sensitive data (yes/no).<br>*If "no," skip to 6.2.e.*<br>*If "yes," complete the remining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the testing results to conclude that all ingress and egress methods enforce secure versions of the (TLS) protocol with end-point authentication prior to the transmission of the sensitive data. | | |

| 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 vendor evidence examined that details whether methods implemented for encrypting sensitive data allow for the use of different types of cryptography or different levels of security. | | |
| | **Indicate** whether the methods implemented to encrypt sensitive data for transmission allow for the use of different types of cryptography or different levels of security (yes/no).<br>*If "no," skip to 6.3.*<br>*If "yes," complete the remining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the testing results to conclude that the 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.<br><br>***Note:*** *The assessor should refer to Control Objective 7 to identify all requirements for appropriate and correct implementation of cryptography.* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Describe** each of the tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor observed in the vendor evidence and test results to conclude that all uses of cryptography for the purpose of securing critical assets is compliant to Control Objective 7. | | | | |
| **6.3.b** Where third-party software or aspects of the execution environment or platform on which the application is run are relied upon for cryptographic services for the protection of sensitive data, the assessor shall examine vendor evidence and test the software to identify these methods and to confirm that the vendor security guidance provides clear and sufficient detail for correctly configuring these methods during the installation of the vendor software.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that details whether the software relies on any third-party software or aspects of the execution environment for cryptographic services to protect sensitive data. | | | | |
| | **Indicate** whether the software relies upon such cryptographic services for the protection of sensitive data (yes/no).<br><br>*If "no," skip to 6.3.c.*<br><br>*If "yes," complete the remining reporting instructions for this test requirement.* | | | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the vendor discovered through software testing to conclude the results of the testing are supported by the vendor evidence. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within that guidance where the correct configuration of such cryptographic services is covered. | | |
| **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 vendor evidence examined that details whether asymmetric cryptography is used for protecting the confidentiality of sensitive data. | | |
| | **Indicate** whether asymmetric cryptography (such as RSA or ECC) is used for protecting the confidentiality of sensitive data (yes/no).<br>*If "no," skip to 7.1.*<br>*If "yes," complete the remining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor discovered through software testing to conclude the results of the testing are supported by the vendor evidence. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results that provides reasonable assurance that private keys are not used for to protect the confidentiality of 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**<br>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**<br>☐ | **N/A**<br>☐ | **Not in Place**<br>☐ |
| **7.1.a** The assessor shall examine the vendor evidence to confirm that, where that cryptography is relied upon (in whole or in part) for the security of the critical assets:<br>• Industry-accepted cryptographic algorithms and modes of operation are used in the software as the primary means for protecting critical assets; and<br>• 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.<br>***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets.* | **Identify** the vendor evidence examined that confirms the findings for 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 (yes/no). | | | | |
| | *If "yes,"* **identify** the unapproved algorithms or modes of operation used and **describe** how they are used in conjunction with approved algorithms in a manner that ensures equivalent cryptographic key strength as 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 model, 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 use of the software as a decryption oracle, brute-force or dictionary attacks against the input domain of the sensitive data, re-use of security parameters such as IVs, or re-encryption of multiple datasets using linearly applied key values (such as XOR'd key values in stream ciphers or one-time pads).<br><br>***Note:*** *The assessor should refer to Control Objective 4 to identify common cryptography attacks.* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that only documented cryptographic algorithms and modes of operation are used in the software. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that each of the cryptographic algorithms and modes of operation in use are implemented correctly (i.e., are fit-for-purpose). | | |
| | **Identify** the protection mechanisms implemented to protect against common cryptographic attacks. | | |
| **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 implementations, and test the software to confirm correct implementations. 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 DSS signature.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that details whether any cryptographic algorithms or modes of operation used by the software require a unique value per encryption operation or session. | | |
| | **Indicate** whether any of the implemented cryptographic algorithms (and their supporting modes of operation) require a unique value per encryption operation or session (yes/no).<br><br>*If "no," skip to 7.1.d.*<br><br>*If "yes," complete the remining 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** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that the cryptographic algorithms and their supporting modes of operation are implemented in such a way that mitigates all known vulnerabilities. | | |
| **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 vendor evidence examined that details whether padding methods are used prior to or during encryption operations. | | |
| | **Indicate** whether padding is used prior to or during encryption operations (yes/no).<br>*If "no," skip to 7.1.e.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that whenever an encryption operation uses padding, it always uses an industry-accepted standard padding method. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **7.1.e** Where hash functions are used within the software, the assessor shall:<br>• Examine publicly available literature and research to identify vulnerable algorithms that can be exploited, and<br>• 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.<br>***Note:*** *The assessor should refer to Control Objective 7.3 to identify secure random number generators.* | **Identify** the vendor evidence that details whether has functions are used within the software. | | |
| | **Indicate** whether hash functions are used (yes/no).<br>*If "no," skip to 7.2.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the testing results to conclude that only approved, collision-resistant hash algorithms and methods are used. | | |
| | **Describe** what the assessor observed in the testing results to conclude that all hash algorithms 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:<br>• 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 application updates) have a unique purpose. For example, no key may be used for both encryption and authentication operations.<br>• 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 of the application (e.g., white-box cryptography).<br>• All cryptographic keys have an equivalent bit strength of at least 128 bits in accordance with industry standards.<br>*(continued on next page)* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | | | |
| | **Describe** what the assessor observed in the testing results to conclude that all cryptographic keys used for providing security to critical assets or other security services to the software have a unique purpose in accordance with the vendor evidence. | | | | |
| | **Describe** what the assessor observed in the testing results to conclude that all keys have defined generation methods, and no secret or private cryptographic keys relied upon for the 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 of the application in accordance with the vendor evidence. | | | | |
| | **Describe** what the assessor observed in the testing results to conclude that All cryptographic keys have an equivalent bit strength of at least 128 bits in accordance with industry standards and the vendor evidence. | | | | |

| 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.<br>• 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).<br>• All keys have a defined generation or injection process, and this process ensures sufficient entropy for the key.<br>• 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 testing results to conclude that 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 in accordance with the vendor evidence. | | |
| | **Describe** what the assessor observed in the testing results to conclude that the integrity and confidentiality of all secret and private cryptographic keys managed by the software are protected when stored in accordance with the vendor evidence. | | |
| | **Describe** what the assessor observed in the testing results to conclude that all keys have a defined generation or injection process, and this process ensures sufficient entropy for the key in accordance with the vendor evidence. | | |
| | **Describe** what the assessor observed in the testing results to conclude that all key-generation functions must implement one-way functions or other irreversible key-generation processes, and no reversible key calculation modes are used to directly create new keys from an existing key in accordance with the vendor evidence. | | |

| 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 vendor evidence examined that details whether cryptography is used for the protection of any cryptographic keys and the effective key strengths provided by such keys. | | |
| | **Indicate** whether cryptography is used to protect any cryptographic keys (yes/no).<br>*If "no," skip to 7.2.c.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of testing are supported by the vendor evidence. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results that demonstrates that all cryptographic keys used to protect other cryptographic keys provide an effective key strength equal or greater to 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:<br>• Key label or name<br>• Key location<br>• Effective and expiration date<br>• Key purpose/type<br>• Key length | **Identify** the vendor evidence examined that details whether public keys are used by the software. | | |
| | **Indicate** whether public keys are used by the system (yes/no).<br>*If "no," skip to 7.2.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that confirms the vendor maintains an inventory of all cryptographic keys in use. | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor discovered through software testing to conclude that the results of the tests are supported by the vendor evidence. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that the authenticity of all public keys used in the software is maintained. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 vendor evidence examined that details whether public or white-box keys are used that are not unique per each software instantiation. | | |
| | **Indicate** whether public or white-box keys are used by the software that are not unique to each software instantiation (yes/no).<br>*If "no," skip to 7.2.e*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that details the methods and procedures implemented by the software to revoke and/or replace such keys (or key pairs). | | |
| | **Describe** each of the software tests performed to confirm that the methods and procedures implemented to revoke and/or replace such keys are supported by the vendor evidence. | | |
| | **Describe** what the assessor discovered through testing to conclude that the results of testing are supported by the vendor evidence. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 (e.g., including it within the scope of FIM systems, protections over private keys, etc.)–is provided in the vendor security guidance documents made available to stakeholders per Control Objective 12. | **Identify** the vendor evidence examined that details whether the software relies upon external files or other data elements for cryptographic key material. | | |
| | **Indicate** whether the software relies upon external files or other data elements for cryptographic key materials (yes/no).<br>*If "no," skip to 7.2.f*<br>*If "yes," complete the remining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that confirms the vendor provides clear and sufficient guidance (in accordance with Control Objective 12) on how to install such key material. | | |
| | **Identify** the page(s) or section(s) within the vendor guidance where the proper installation of such key material is covered. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 limitation of execution environment), the assessor shall confirm that the methods implemented are appropriate to protect the public keys. | **Identify** the vendor evidence that details whether public keys are used by the software, and whether such keys are manually loaded or used as root keys. | | |
| | **Indicate** whether any public keys used by the software are manually loaded or used as root keys (yes/no).<br>*If "no," skip to 7.2.g*<br>*If "yes," complete the remining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed to confirm that the public keys are installed and stored in a way that provides dual control. | | |
| | **Indicate** whether vendor evidence examination or the results of software testing indicate that complete dual control of manual key loading or usage is infeasible (yes/no).<br>*If "no," skip to 7.2.g.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** the circumstances that make the implementation of complete dual control infeasible. | | |
| | **Describe** the methods implemented to protect the public keys and why they are appropriate for that purpose. | | |

| 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 vendor evidence examined that details how all secret and private keys are managed. | | |
| | **Describe** each of the software tests performed to confirm the methods implemented by the software to manage secret and private keys are implemented in a way that ensures split knowledge over the key. | | |
| | **Indicate** whether vendor evidence examination or the results of software testing indication absolute split knowledge of the secret/private keys is infeasible (yes/no).<br>*If "no," skip to 7.2.h.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** the circumstances that make the implementation of split knowledge infeasible. | | |
| | **Describe** the methods implemented to protect secret and/or private keys and why the protection methods are reasonable for their intended purpose. | | |

| 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) in line with the requirements of this standard. | **Identify** the vendor evidence examined that details the methods implemented by the software to "roll" any keys at the end of their crypto-period. | | |
| | **Describe** each of the software tests performed to confirm the methods implemented by the software to "roll" any keys at the end of their crypto-period are implemented in a manner consistent with the vendor evidence. | | |

| 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:<br>• Use at least 128 bits of entropy prior to the output of any random numbers from the random number generator.<br>• 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 vendor evidence examined that confirms all random number generation methods implemented in the software are implemented in a manner consistent with this test requirement. | | | | |
| | **Describe** what the assessor observed in the vendor evidence that demonstrates 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 vendor evidence that provides reasonable assurance that sufficient entropy (i.e., at least 128 bits) is always provided or produced upon start-up or entry of other predicable states of the system. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 require seeding from an external entropy source to correctly output random data. | **Identify** the vendor evidence examined that details whether any random number generators or "seeds" used by the software rely on a previous assessment to meet this control objective. | | |
| | **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).<br>*If "no," skip to 7.3.c.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that details the scope of the previous assessment (and approval). | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that correct areas of the software were included in the previous assessment of the random number generator, and that all vendor claims do not exceed the scope of evaluation or approval of that software. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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.<br><br>Where problems are known, but have been mitigated by the application vendor, the assessor shall examine vendor evidence and test the software to confirm that the vulnerabilities have been sufficiently mitigated.<br><br>The assessor shall test the software to confirm that third-party software, platforms, or libraries are correctly integrated, implemented, and configured.<br><br>*(continued on next page)* | **Identify** the vendor evidence that details whether third-party software, platforms or libraries are used for all or part of the random number generation process. | | |
| | **Indicate** whether third-party software, platforms, or libraries are used for all or part of the random number generation process (yes/no).<br><br>*If "no," skip to 7.3.e.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement and 7.3.d.* | | |
| | **Identify** the publicly-available literature examined to determine whether known problems (i.e., vulnerabilities) exist in the third-party software, platforms or libraries used for random number generation. | | |
| | **Indicate** whether any known problems were identified (yes/no).<br><br>*If "no," skip to 7.3.d.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed to confirm that protection mechanisms have been implemented to mitigate the known vulnerabilities. | | |
| | **Describe** what the assessor observed in testing results to conclude that the vulnerabilities have been sufficiently mitigated. | | |

| 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 testing results to conclude that the third-party software, platforms or libraries used for random number generation have been integrated, implemented, and configured correctly. | | |
| **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 application is executed. | **Identify** the vendor evidence examined that details all of the methods implemented by the software to prevent or detect the interception or "hooking" of random number calls serviced from third-party software or from the software's execution environment. | | |
| | **Describe** each of the software tests performed to confirm the methods implemented by the software are consistent with the vendor evidence. | | |
| **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.<br><br>***Note:*** *The assessor can use the NIST Statistical Test Suite to identify statistical correlation in the random number generation implementation.* | **Describe** each of the tests performed in support of this test requirement, including 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 testing results to conclude that there is reasonable assurance 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 generators ensures 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 DSS, etc.) have entropy that meets the minimum effective strength requirements of the cryptographic primitives and keys.<br><br>***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets, including keys and other cryptographic material.* | **Identify** the vendor evidence examined that details the methods used for the generation of all cryptographic keys and other key materials, and the effective strength requirements for all cryptographic primitives and keys. | | | | |
| | **Describe** each of the software tests performed to confirm the methods implemented by the software for the generation of all cryptographic keys and other materials is consistent with the vendor evidence. | | | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that the methods used for generation of all cryptographic keys and other material have entropy that meets the minimum effective strength requirements of the cryptographic primitives and keys.<br><br>***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 application, 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:<br>• 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).<br>• 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.<br>• Clear and sufficient guidance is provided in the vendor security guidance made available to stakeholders (per Control Objective 12) that any passphrase used must be:<br>*(continued on next page)* | **Identify** the vendor evidence examined that details how cryptographic keys are generated by the software. | | |
| | **Indicate** whether any cryptographic keys are generated through processes that require direct user interaction with the application (yes/no).<br>*If "no," skip to 7.4.c.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed in support of this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that any methods used for generating 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 vendor evidence and testing results to conclude that the password/passphrase is passed through an industry-standard key-derivation function which provides a work factor of at least 10,000. | | |

| | | |
|---|---|---|
| ○ Randomly generated itself, using a valid and secure random process: an online random number generator must not be used for this purpose.<br>○ 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 (For example, for an AES128 key, 2 people must each enter 32 hex characters or 3 people must enter at least 16 hex characters each). | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where stakeholders are instructed to use passwords/passphrases that are randomly generated using a valid and secure random process. | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where stakeholders are instructed that passwords/passphrases must never be implemented in a way that violates requirements for split knowledge. | |
| **7.4.c** Where any third-party software or platforms are relied upon by the software application 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 is provided in the vendor security guidance made available to stakeholders (per Control Objective 12) on the secure configuration and usage of these software components.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that details whether third-party software or platforms are relied upon by the software for the generation of all cryptographic keys and other material, but do not meet entropy requirements. | |
| | **Indicate** whether sufficient entropy could not be provided per Test Requirement 7.4.a (yes/no).<br>*If "no," skip to 8.1.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | |
| | **Identify** the vendor evidence examined that details the mitigations implemented to compensate for the lack of sufficient entropy. | |

| 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 to confirm the mitigations implemented are consistent with the vendor evidence. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that mitigations implemented are sufficient to compensate for the lack of sufficient entropy. | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where the secure configuration and usage of any such mitigations is covered. | | |

## Security Objective: 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**<br>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.**<br>***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**<br>☐ | **N/A**<br>☐ | **Not in Place**<br>☐ |
| **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.<br>***Note****: The assessor should refer to Control Objective 1 to identify all critical assets.* | **Identify** the vendor evidence examined that details all mechanisms used by the software to track all access and usage of critical assets. | | | | |
| | **Describe** each of the software tests performed to confirm that the mechanisms implemented by the software to track all access and usage of critical assets are consistent with the vendor evidence. | | | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude 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. | | | | |

| 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:<br>• Enablement of any privileged modes of operation<br>• Disabling of encryption of sensitive data<br>• Decryption of sensitive data<br>• Exporting of sensitive data to other systems or processes<br>• Failed authentication attempts<br>• Disabling or deleting a security control or altering security functionality | **Identify** the vendor evidence examined that demonstrates that the tracking methods implemented track the specific activities defined within this test requirement. | | | | |
| | **Describe** each of the software tests performed to confirm the tracking methods implemented are consistent with the vendor evidence.<br>***Note**: it is expected that a software test would be performed for each of the bulleted items in the test requirement.* | | | | |
| **8.2.b** The assessor shall examine vendor evidence and test the software to confirm that the tracking method(s) implemented provide:<br>• A unique identification for the person, system, or entity performing the access<br>• A timestamp for each tracked event<br>• Details on what critical asset has been accessed | **Identify** the vendor evidence examined that demonstrates the tracking methods implemented capture, at a minimum, the information specified in this test requirement. | | | | |
| | **Describe** each of the software tests performed to confirm the tracking methods implemented capture information in a manner consistent with what was specified the vendor evidence. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **8.2.c** The assessor shall test the software to confirm that sensitive data is not directly recorded in the tracking data. | **Describe** each of the software tests performed to determine whether sensitive data is recorded in tracking data. | | |
| | **Describe** what the assessor observed in the testing results that provides reasonable assurance that sensitive data is not recorded in activity tracking data. | | |

| 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 vendor evidence examined that details whether activity records are managed by the software. | | | | |
| | **Indicate** whether the software manages the activity records (yes/no).<br>*If "no," skip to 8.3.b.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | | | |
| | **Identify** the vendor evidence examined that details all of the protection methods implemented to protect the completeness, accuracy, and integrity of the activity records. | | | | |
| | **Describe** each of the software tests performed to confirm that that the protection mechanisms implemented by the software are consistent with the vendor evidence. | | | | |
| | **Summarize** each of the protection methods implemented by the software to protect the completeness, accuracy and integrity of 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 vendor security guidance made available to stakeholders (per Control Objective 12).<br><br>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 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.<br><br>***Note:*** *The assessor should refer to Control Objective 1 to identify all critical assets.* | **Identify** the vendor evidence examined that details whether the software utilizes other systems for maintaining tracking data. | | |
| | **Indicate** whether the software utilizes (or supports the use of) other systems for the maintenance of tracking data, such as a log server (yes/no).<br><br>*If "no," skip to 8.4.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where the correct and complete setup and/or integration of such log storage system(s) is covered. | | |
| | **Describe** each of the software tests performed to identify the methods implemented by the software to secure the authenticity of tracking data during transmission to the log storage system(s). | | |
| | **Describe** what the assessor observed in the testing results to conclude that the methods implemented meet all applicable requirements of this standard. | | |

| 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:<br>• The software does not overwrite existing tracking data upon a restart of the software. Each new start shall only append to existing datasets, or create a new tracking dataset.<br>• Where unique dataset names are relied upon for maintaining integrity between execution instances, the implementation ensures that another application (including another instance of the same application) cannot overwrite or render invalid existing datasets.<br>*(continued on next page)* | **Identify** the vendor evidence examined that details how the software protects the integrity of activity tracking records, and confirms those methods are implemented in a manner consistent with this test requirement. | | | | |
| | **Describe** each of the software tests performed to confirm the methods implemented by the software are consistent with the vendor guidance and this test requirement. | | | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude 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. | | | | |
| | **Indicate** whether unique dataset names are relied upon for maintaining the integrity between execution instances (yes/no). | | | | |
| | *If "yes,"* **describe** what the assessor observed in the vendor evidence and testing results to conclude that no another application (or instance of the same application) can overwrite or render invalid any existing data sets. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| • 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. | **Indicate** whether conditions exist where it is not possible for the software to apply file privileges to assist with maintaining the integrity of the activity tracking data set (yes/no). | | |
| | *If "no,"* **describe** what the assessor observed in the vendor evidence and testing results to conclude that the software applies suitable file privileges to assist with maintaining the integrity of the tracking dataset. | | |
| | *If "yes,"* **describe** the vendor's justification for why such file privileges could not be applied. | | |
| | *If "yes,"* **identify** the additional mitigations implemented to maintain the integrity of the 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):<br>• Performing actions that should be tracked, force-closing and then restarting the software, and performing other tracked actions.<br>• 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.<br>• 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.<br>• 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).<br>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.<br>*(continued on next page)* | **Describe** how each of the software tests defined in this test requirement were performed and the results of each test. | | |
| | **Indicate** whether any of the tests specified in this test requirement could not be performed (yes/no).<br>*If "no," skip to 9.1.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the software tests specified in this test requirement that could not be performed. | | |
| | For each of the software tests not performed, **identify** the individuals interviewed that confirm the vendor maintains reasonable justification to describe why this is the case. | | |
| | For each of the software tests not performed, **describe** the vendor's justification for why they could not be performed. | | |
| | For each of the software tests not performed, **identify** each of the protections put in place to prevent such scenarios from affecting the integrity of the tracking records. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| | For each of the software tests not performed, **describe** what the assessor observed in the vendor evidence and testing results to conclude that the protections put in place are appropriate to prevent the scenario described from affecting the integrity of the 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**<br>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).<br><br>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, and shall test the software to confirm controls are implemented to minimize the associated risk.<br><br>***Note:*** *The assessor should refer to Control Objective 4 for information on the possible attack scenarios and mitigation controls implemented by the software vendor.*<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that details the methods implemented by the software to validate the integrity of its own executable and any configuration options, files or datasets the software relies upon for operation. | | | | |
| | **Describe** each of the software tests performed to confirm the methods implemented by the software are consistent with the vendor evidence, and ensure unauthorized, post-deployment changes are detected. | | | | |
| | **Indicate** whether the execution environment prevents the software from validating the integrity of its own executable and any configuration options, files, and datasets that it relies upon for operation (yes/no).<br><br>*If "no," skip to 9.1.b.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | | | |
| | **Identify** the vendor evidence and publicly-available literature examined that confirms there are no methods made available by the platform for validating the integrity/authenticity of the software executables, configuration files, and datasets. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| | **Identify** the vendor evidence examined that details all of the additional controls implemented by the software to protect the integrity of the software's executables and the configuration options, files, and datasets 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 application and dataset(s) upon which it relies for secure operation are checked upon execution of the application, 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 vendor evidence examined that demonstrates how the software checks integrity values used by the software and the datasets upon which the software relies for its secure operation in a manner consistent with this test requirement. | | |
| | **Describe** each of the software tests performed to confirm the software checks implemented by the software are consistent with this test requirement and the vendor evidence. | | |
| | **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 action the software takes upon the failure of such integrity checks. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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.<br>*Note: The assessor should refer to Control Objective 7 for information on appropriate and correct usage of cryptography.* | **Identify** the vendor evidence examined that details whether cryptographic primitives are used by the software for anomaly-detection. | | |
| | **Indicate** whether cryptographic primitives are used by the software for anomaly-detection (yes/no).<br>*If "no," skip to 9.1.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that details how cryptographic primitives are protected. | | |
| | **Describe** each of the software tests performed to confirm the protection mechanisms implemented are consistent with the vendor evidence. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that the protection mechanisms implemented are appropriate for protecting cryptographic primitives | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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 protected as sensitive information.<br><br>***Note:*** *The assessor should refer to Control Objective 1 and 6 to identify all critical assets and implemented security controls.* | **Identify** the vendor evidence examined that details whether stored values are used by the software for anomaly-detection. | | |
| | **Indicate** whether stored values are used by the software for anomaly-detection (yes/no).<br><br>*If "no," skip to 9.1.e.*<br><br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that details how stored values are protected. | | |
| | **Describe** each of the software tests performed confirm the protection mechanisms implemented are consistent with the vendor evidence. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that the protection mechanisms implemented are appropriate to protect the stored values are appropriately protected. | | |

| 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 update. | **Identify** the vendor evidence examined that details whether configuration or other dataset values are 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).<br>*If "no," skip to 9.1.f.*<br>If "yes," complete the remaining reporting instructions for this test requirement. | | |
| | **Identify** the vendor evidence examined that details the integrity protections implemented to protect configuration or other dataset values. | | |
| | **Describe** each of the software tests performed to confirm that the integrity protections are implemented in a manner consistent with the vendor evidence. | | |
| | **Describe** how the integrity protections are implemented in a way that allow for updates during execution while still ensuring the integrity of the values can be validated after 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 vendor evidence examined that details the controls implemented by the software to prevent brute-force attacks on account, password, or cryptographic-key input fields. | | |
| | **Describe** each of the software tests performed to confirm the controls implemented by the software are consistent with the vendor evidence. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that the controls implemented are appropriate to prevent brute-force attacks on account, password, or cryptographic-key input fields. | | |

## Security Objective: 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**<br>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 has identified common methods for attack against the software product. This may include platform-level, protocol-level, and/or language-level attacks. | **Identify** the vendor evidence examined that details all common 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 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 vendor evidence examined in Test Requirement 10.1.a to conclude that the vendor has reasonably considered the susceptibility of the software to common attack methods. | | | | |
| **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.<br>*(continued on next page)* | **Identify** the vendor evidence examined that the controls implemented by the software to mitigate each of the attacks identified in Test Requirement 10.1.a. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that protection mechanisms are appropriate for mitigating each of the attacks identified in Test Requirement 10.1.a. | | | | |

| 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 vendor evidence to conclude that the vendor's software release process confirms that such mitigations are (and remain) in place. | | |

| 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.<br><br>***Note:*** *The assessor should refer to Control Objective 4 for information on the possible attack scenarios and mitigation controls implemented by the software vendor.* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Summarize** the testing processes implemented by the vendor to validate the mitigations used to secure the software against attacks. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that such processes are performed throughout the entire software lifecycle. | | | | |
| **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:<br>• Includes, at a minimum, the use of automated tools capable of detecting vulnerabilities both in software code and during software execution, and that the tools used for security testing are appropriate for detecting applicable vulnerabilities and are suitable for the software architecture, development languages, and frameworks used in the development of the software.<br><br>*(continued on next page)* | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Identify** the automated tools used as part of the vendor's testing process to detect vulnerabilities in software code and during execution in accordance with this test requirement. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the vendor's testing process accounts for the entire code base, including third-party, open-source, or shared components and libraries. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| • Accounts for the entire code base, including detecting vulnerabilities in third-party, open-source, or shared components and libraries.<br>• Accounts for common vulnerabilities and attack methods.<br>• Demonstrates a history of finding software vulnerabilities and remediating them prior to retesting of the software. | **Describe** what the assessor observed in the vendor evidence to conclude that the vendor's testing process accounts for common vulnerabilities and attack methods. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the vendor's testing process demonstrates a history of finding software vulnerabilities and remediating them prior to retesting of the software. | | |
| **10.2.c** Where vendor evidence shows the release of software with known vulnerabilities, the assessor shall examine vendor evidence to confirm that:<br>• The vendor implements an industry-standard vulnerability-ranking system (such as CVSS) that allows for the categorization of vulnerabilities.<br>• 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 vendor evidence examined that confirms the findings for this test requirement. | | |
| | **Describe** the vendor's vulnerability ranking/categorization scheme and how it aligns with other industry-standard schemes. | | |
| | **Describe** the vendor's process for ensuring 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**<br>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:<br>• Reasonable criteria exist for releasing software updates to fix security vulnerabilities.<br>• Security updates are made available to stakeholders in accordance with defined criteria. | **Identify** the vendor evidence examined that confirms the findings for this test requirement. | | | | |
| | **Describe** the vendor's criteria for how (and how often) the vendor releases software updates to fix security vulnerabilities and why the assessor considers the criteria reasonable. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude the vendor makes security updates available to stakeholders in accordance with its defined criteria. | | | | |
| **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.<br>*(continued on next page)* | **Identify** the vendor software updates sampled for this test requirement. | | | | |
| | **Identify** the vendor evidence examined, including update-specific security testing results and details, that confirm the findings for this requirement. | | | | |
| | **Indicate** whether any evidence was obtained that demonstrates the vendor did not provide security fixes to stakeholders in accordance with its defined criteria (yes/no). | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| | *If "no,"* **describe** what the assessor observed in vendor evidence to conclude that software updates made available to stakeholders include security fixes to address vulnerabilities in the software in accordance with defined criteria | | |
| | *If "yes,"* **describe** the vendor's justification for not providing security fixes in accordance with its' defined criteria and why the assessor considers this reasonable. | | |

| 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 vendor security guidance made available to stakeholders (per Control Objective 12). | **Identify** the vendor evidence examined that details how software updates are released in a manner that protects the integrity of the software code during transmission and install. | | | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the vendor's methods for delivering software updates are appropriate to 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 code (yes/no).<br>If "no," skip to 11.2.b.<br>If "yes," complete the remaining reporting instructions for this test requirement. | | | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where instructions are provided to guide users through this process. | | | | |

| 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 vendor evidence examined that details whether methods to protect the integrity of update code are not cryptographically secure. | | |
| | **Indicate** whether the methods to protect the integrity of update code are cryptographically secure (yes/no). | | |
| | *If "yes,"* **describe** what the assessor observed in the vendor evidence to conclude integrity methods are cryptographically secure. | | |
| | *If "no,"* **describe** how the vendor evidence examined 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 vendor informs users of the software updates and provides clear and sufficient guidance on how they may be obtained and installed (per Control Objective 12). | **Identify** the vendor evidence examined that that demonstrates the vendor informs users (and other stakeholders) of the availability software updates. | | |
| | **Identify** the vendor evidence examined that demonstrates the vendor provides guidance on how software updates should be obtained and installed, in accordance with Control Objective 12. | | |
| | **Identify** the page(s) or section(s) within the vendor guidance where the appropriate acquisition, and installation or implementation of software updates is covered. | | |

| 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 vendor evidence examined that details the vendor's process for notifying users when known vulnerabilities in the software have been identified but not yet patched in the software. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the vendor's process includes methods to provide users with mitigation techniques for unpatched vulnerabilities until a security patch can be provided. | | |
| **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 vendor evidence examined that confirms the findings for this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence to conclude that the 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: Vendor Security Guidance**<br>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 vendor evidence examined that details the vendor's process for providing stakeholders guidance on the secure installation and use of the software. | | | | |
| **12.1.b** The assessor shall examine vendor evidence to confirm that the guidance:<br>• Includes details on how to securely and correctly install any third-party software that is required for the operation of the vendor software.<br>• 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).<br>• Includes instructions for key management (e.g., use of keys, how keys are distributed, loaded, removed, changed, destroyed, etc.)<br>*(continued on next page)* | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where the installation or implementation of any third-party software required for software operation is covered. | | | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where instructions for the proper configuration of the platform(s) on which the software will be executed are provided. | | | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where instructions for the proper management of cryptographic keys are covered. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| • 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.<br>• Does not instruct the user to execute the software in a privileged mode higher than what is required by the software.<br>• 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.<br>• 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 vendor guidance to reasonably conclude that users are not instructed to disable security settings or parameters within the installed environment to facilitate software operation. | | |
| | **Describe** what the assessor observed in the vendor guidance to reasonably conclude that users are not instructed to execute the software in a privileged mode higher than the minimum privileges necessary for software operation. | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where instructions on how to validate the version of the software and details on the version of the software the guidance applies to are covered. | | |
| | **Describe** what the assessor observed in vendor evidence to conclude that the vendor provides justification(s) for all requirements within this standard deemed not applicable, and why the assessor considers each of the justification(s) reasonable. | | |

## Security Objective: 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**<br>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**<br>☐ | **N/A**<br>☐ | **Not in Place**<br>☐ |
| **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 vendor evidence examined (as identified in the testing of Control Objective 1) that details all locations within the software (or its execution environment) where sensitive data is stored (both persistently and temporarily). | | | | |
| | **Describe** each of the software tests performed identify all locations within the software (or its execution environment) where sensitive data is stored. | | | | |
| | **Describe** what the assessor observed in the test results (and vendor evidence) that provides reasonable assurance the software does not store sensitive authentication data after authorization.<br>***Note**: If the software does store sensitive authentication data after authorization, then A.1.1.b must be completed.* | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **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. | **Indicate** whether the testing in A.1.1.a determined the software stores sensitive data after authorization (yes/no).<br>*If "no," skip to A.2.1.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Identify** the vendor evidence examined that demonstrates 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**<br>Protect stored cardholder data. | | | | | |
| **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**<br>☐ | **N/A**<br>☐ | **Not in Place**<br>☐ |
| **A.2.1.a** The assessor shall examine the instructions prepared by the software vendor and confirm the documentation includes the following guidance for customers, integrators and resellers:<br>• A list of all locations where the software stores cardholder data.<br>• Instructions on how to securely delete cardholder data stored by the payment application, including data stored on underlying software or systems (such as OS, databases, etc.).<br>• 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 vendor evidence examined that demonstrates the vendor provides stakeholders guidance consistent with this test requirement. | | | | |
| | **Identify** the vendor guidance and the page(s) or section(s) within the guidance that details the locations where the software stores cardholder data. | | | | |
| | **Identify** the vendor guidance and the page(s) or section(s) within the guidance where instructions on how to securely delete cardholder data stored by the software are provided. | | | | |
| | **Identify** the vendor guidance and the page(s) or section(s) within the guidance where instructions for configuring the underlying software or systems to prevent inadvertent capture or retention of cardholder data are provided. | | | | |

| 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 security guidance made available to stakeholders (per Control Objective 12), to confirm the guidance includes the following instructions for customers and integrators/resellers:<br>• Details of all instances where PAN is displayed.<br>• Confirmation that the payment software masks PAN to display a maximum of the first six and last four digits by default on all displays.<br>• 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 vendor evidence examined that confirms the vendor provides guidance to stakeholders in a manner consistent with this test requirement. | | | | |
| | **Identify** the vendor guidance, and the page(s) or section(s) within the guidance where all instances where PAN is displayed within the software (or its execution environment) are detailed. | | | | |
| | **Identify** the vendor guidance, and the page(s) or section(s) within the guidance where customers and integrators/resellers are instructed that all displays of PAN must be masked to a maximum of the first six and last four digits by default. | | | | |
| | **Indicate** whether the software supports the display of full PAN (yes/no). | | | | |
| | *If "yes,"* **identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where instructions for how to properly configure the software to display more than the first six and last four digits of the PAN are provided.<br>***Note**: If "yes," A.2.2.c applies as well.* | | | | |

| 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. | **Describe** each of the software tests performed to identify all locations within the software where PAN is displayed. | | |
| | **Describe** what the assessor observed in the testing results to conclude 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. | ***Note**: This test requirement is only applicable where the software supports the display of the full PAN.*<br>**Describe** each of the software tests performed to determine whether the guidance provided in Test Requirement A.2.2.a on properly configuring the software to display more than the first six/last four digits is accurate. | | |
| | **Describe** what the assessor observed in the vendor evidence (examined in Test Requirement A.2.2.a) and the testing results to conclude that the instructions provided in the vendor guidance for displaying more that the first six/last four digits are accurate. | | |

| 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:**<br>• **Truncation (hashing cannot be used to replace the truncated segment of PAN).**<br>• **Index tokens and pads (pads must be securely stored).**<br>• **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 security guidance made available to stakeholders (per Control Objective 12) to verify the guidance includes the following:<br>• 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 application (per as identified in Control Objective A.2.1).<br>• 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.<br>*(continued on next page)* | **Identify** the vendor evidence examined that confirms the vendor provides security guidance to stakeholders in a manner consistent with this test requirement. | | | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where instructions for properly configuring all available options to render cardholder data unreadable are provided. | | | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance that details all instances where cardholder data is output for the purposes of storing outside of the payment software. | | | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| • 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 vendor guidance examined, and the page(s) or section(s) within the guidance where instructions are provided to remind users that they are responsible for rendering PAN unreadable wherever it is output for the purposes of storing outside of the payment software. | | |
| | **Identify** the vendor guidance examined, and the page(s) or section(s) within the guidance where instructions are provided to remind users that wherever debugging logs are enabled that might include PAN, that the debugging logs must be protected from authorized access, disabled as soon as troubleshooting is complete, and securely deleted when no longer needed. | | |
| **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:<br>• Truncation<br>• Index tokens and pads, with the pads being securely stored<br>• Strong cryptography, with associated key-management processes and procedures.<br>***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 vendor evidence examined that details all methods used to protect PAN during persistent storage. | | |
| | **Describe** each of the software tests performed to confirm the methods implemented by the software to protect PAN are consistent with the vendor evidence and this test requirement. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that PAN is rendered unreadable wherever it is stored persistently. | | |

| Control Objective and Test Requirements | Reporting Instructions | Reporting Details: Assessor's Response | Summary of Assessment Findings (check one) |
|---|---|---|---|
| **A.2.3.c** Where software creates both tokenized and truncated versions of the same PAN, the assessor shall test the software to confirm that the tokenized and truncated versions cannot be correlated to reconstruct the original PAN. | **Identify** the vendor evidence examined that details whether the software creates both tokenized and truncated versions of the same PAN. | | |
| | **Indicate** whether the software creates both tokenized and truncated versions of the same PAN (yes/no).<br>*If "no," skip to A.2.3.d.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed to try and correlate the tokenized and truncated versions of the PAN to reconstruct the original PAN. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results that provides reasonable assurance 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 vendor evidence examined that details whether the software creates or generates files for use outside of the software. | | |
| | **Indicate** whether the software creates or generates files for use outside the software (yes/no).<br>*If "no," skip to A.2.3.e.*<br>*If "yes," complete the remaining reporting instructions for this test requirement.* | | |
| | **Describe** each of the software tests performed to determine whether PAN is rendered unreadable anywhere it is output by the software. | | |
| | **Describe** what the assessor observed in the vendor evidence and testing results to conclude that PAN is rendered unreadable wherever it is output outside of the software. | | |
| **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 vendor evidence examined that details whether the vendor stores PAN on vendor systems for any reason. | | |
| | **Indicate** whether the software vendor stores PAN on vendor systems for any reason (yes/no). | | |
| | *If "yes,"* **describe** each of the software tests performed in support of this test requirement. | | |
| | *If "yes,"* **describe** what the assessor observed in the vendor evidence and testing results to conclude that all PAN stored on vendor systems is rendered unreadable. | | |

# 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 5.5.1 of the *Secure Software Standard Program Guide*. This confirmation must be submitted to PCI SSC along 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 5.5.1 of the *Secure Software Program Guide*, was used for this assessment.<br>***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:*<br>***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. | |