Security Standards Council®

Payment Card Industry (PCI)

Software Security Framework

Secure Software Lifecycle
Template for Report on Compliance

Version 1.1
February 2021

Document Changes

Date	Version	Description
September 2019	1.0	Initial release of Report on Compliance (ROC) template for the *PCI Secure Software Lifecycle Requirements and Assessment Procedures version 1.0*.
February 2021	1.1	Updates to align with changes from *PCI Secure Software Lifecycle Requirements and Assessment Procedures* version 1.0 to 1.1. Also includes minor corrections and edits made for clarification and/or formatting purposes and to address errata.

Table of Contents

Introduction to the PCI Secure SLC ROC Reporting Template

This document, the *PCI Software Security Framework – Secure Software Lifecycle Template for Report on Compliance* (hereinafter referred to as the "Secure SLC ROC Reporting Template") is for use with the *PCI Software Security Framework – Secure Software Lifecycle Requirements and Assessment Procedures* ("PCI Secure SLC Standard") *Version 1.1* and is the mandatory template for Secure SLC Assessors completing a Secure SLC Assessment. The Secure SLC ROC Reporting Template provides reporting instructions and a reporting template for Secure SLC Assessors. Using this template assures a consistent level of reporting against the PCI Secure SLC Standard amongst assessors.

Use of this Reporting Template is mandatory for all Secure SLC 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 they complete reporting, but also provide context for the report recipient(s). The inclusion of additional text or sections is permitted within reason, as noted above.

A Secure SLC 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 SLC Report on Compliance (ROC) 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 SLC ROC provides a comprehensive summary of testing activities performed and information collected during the Secure SLC Assessment. The information contained in a Secure SLC ROC must provide enough detail and coverage to support the assessor's opinion that the Secure SLC Qualified Software Vendor has met all control objectives within the PCI Secure SLC Standard.

This template should be used in conjunction with appropriate 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 Lifecycle Requirements and Assessment Procedures*
- *Software Security Framework – Secure Software Lifecycle Program Guide*
- *Software Security Framework – Secure Software Lifecycle Attestation of Compliance*
- *Software Security Framework – Glossary of Terms, Abbreviations, and Acronyms*
- *Software Security Framework – Qualification Requirements for Assessors*

Secure SLC ROC Reporting Template Sections

The Secure SLC ROC Reporting Template includes the following sections:

1. Contact Information and Report Summary
2. Scope of the Secure SLC Assessment
3. Secure SLC Assessment Details
4. Assessor Company Attestations
5. Findings and Observations

The Secure SLC ROC Reporting Template also includes the following Appendix:

A. Additional Information Worksheet

All numbered sections must be thoroughly and accurately completed. Use of Appendix A (or any additional appendicies defined by the Assessor) is optional.

The Secure SLC ROC Reporting Template contains instructions to help ensure that Secure SLC 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 vendor.

Documenting the Assessment Findings and Observations

Within the “Findings and Observations” section of the Secure SLC ROC Reporting Template is where the detailed results of the 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 Findings”) 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 ROC, as well as consistent with other related reporting materials such as the Attestation of Compliance (AOC).

Table 2: Selecting the Appropriate Compliance 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 SLC 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 SLC 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 what the assessor observed in the vendor evidence to conclude that security control effectiveness is monitored throughout the entire software lifecycle.	The response would include a detailed description of the item or activity in question – for example, details of how the evidence examined or individuals interviewed demonstrate a control objective was met, or how the assessor concluded a control implemented by the vendor is fit-for-purpose. The response should be of sufficient detail to provide the reader with a comprehensive understanding of the item or activity being described.
Identify	Identify the vendor evidence examined.	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 sensitive production data was found on vendor systems (yes/no).	The response would be either "yes" or "no". ***Note****: The applicability of some reporting instructions may be dependent on the response of a previous reporting instruction. For example, a response of "yes" to a question about a Secure SLC process may result in further details being requested about that particular process. If applicable, the reporting instruction will direct the assessor to a subsequent instruction based on the yes/no answer.*
Summarize	Summarize how the vendor prevents previously resolved vulnerabilities or similar vulnerabilities from being reintroduced into software.	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 SLC 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 SLC 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 SLC Standard were used, and describe how those assessment procedures provide at least the same level of assurance that would have been achieved using the stated test requirements.

Reporting Expectations

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

Dependence on Third-Party Compliance

A Vendor’s Secure SLC process may require or utilize one or more products or services provided by third-parties (e.g., unrelated companies that perform software development services, code reviews, testing of software, and/or other services). Such third-parties are considered “Third-Party Service Providers” with respect to the Vendor’s Secure SLC processes, and their products and services—to the extent required, utilized, or incorporated into or as part of the Vendor’s Secure SLC processes—shall be assessed as part of Vendor’s Secure SLC Assessment.

For a given Secure SLC Assessment, the supporting Third-Party Service Provider product(s) or service(s) are considered part of the Vendor’s overall Secure SLC processes and are assessed as part of the Vendor’s entire secure software lifecycle process assessment.

Use of Sampling During Testing

Where appropriate or instructed, Secure SLC Assessors may utilize sampling as part of the testing process. If sampling is used, the Secure SLC Assessors must specify each sample used in section 3.3 of the Secure SLC ROC 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 3.3.

Using the Appendix

The Secure SLC ROC Reporting Template includes Appendix A: Additional Information Worksheet which can 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 SLC Assessor’s findings. Any information recorded in Appendix A should reference back to the applicable Secure SLC Standard control objectives and test requirements.

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

Template for PCI Secure SLC Report on Compliance

This template is to be used for creating a Secure SLC Report on Compliance. Content and format of the ROC 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 Lifecycle Assessor Contact Information			
Assessor company name:		Assessor name:	
Assessor e-mail:		Assessor phone number:	
Confirmation that internal QA was fully performed on the entire submission per requirements in the relevant program documentation.	☐ Yes ☐ No *Note: If "No," this is not in accordance with PCI Program requirements.*	QA reviewer name:	
		QA reviewer phone number:	
		QA reviewer e-mail address:	

1.2 Date and Timeframe of Assessment

Date of report: ***Note***: *This date must be shown as the "Secure SLC ROC Completion Date" in Part 3d of the Secure SLC AOC.*	
Timeframe of assessment (start date to completion date):	
Identify date(s) spent onsite at the Software Vendor, if applicable:	
Describe how time was spent onsite at the Software Vendor, how time was spent performing remote assessment activities, and how time was spent on validation of remediation activities: ***Note***: *Provide range of dates for each activity.*	

1.3 PCI Secure SLC Version

Version of the PCI Secure SLC Standard used for this assessment:	

2. Scope of the Secure SLC Assessment

2.1 Business Units and Locations Covered		
Describe all of the software vendor's business units and locations that were covered under this Secure SLC Assessment:		
Business Unit Name:	***Business Location Name:***	***Address** (Street, City, State/Country, etc.):*

2.2 Software Product Categories Covered			
Describe all of the software product categories covered under this Secure SLC Assessment (check all that apply): ***Note**: See Section A.3 in the PCI Secure Software Lifecycle Program Guide for a detailed explanation of product categories and how they are used.*			
☐ (01) POS Suite/General	☐ (02) Payment Middleware	☐ (03) Payment Gateway/Switch	☐ (04) Payment Back Office
☐ (05) POS Admin	☐ (06) POS Specialized	☐ (07) POS Kiosk	☐ (08) POS Face-to-Face/POI
☐ (09) Shopping Cart / Store Front	☐ (10) Card-Not-Present	☐ (11) Automated Fuel Dispenser	☐ (12) Payment Component
☐ Other (please explain):			

2.3 PCI-Validated Payment Software Covered	
Does the Software Vendor have any payment software validated to the PCI Secure Software Standard that is covered under this Secure SLC Assessment?	☐ Yes ☐ No

If "Yes," describe all of the validated payment software covered under this Secure SLC Assessment:

Validated Payment Software Name:	***PCI Identifier:***	***Product Category:***

2.4 Third-Party Service Provders	
Does the Software Vendor outsource any software lifecycle functions to third-party service providers? ***Note****: Third-party service providers are those entities with whom the Software Vendor has established contractual agreements to govern services provided by the third-party to the Software Vendor. This <u>does not</u> include open-source software providers whose software is incorporated into the Software Vendor's payment software.*	☐ Yes ☐ No

If "Yes," identify and describe all of the third-party providers and the services employed by the Software Vendor:

Third-Party Company Name	***Description of Third-Party Services Provided to Software Vendor***	***Secure SLC Control Objectives Applicable to Third-Party Services Provided***	***Description of How Third-Party Compliance Was Validated by the Secure SLC Assessor***

3. Secure SLC Assessment Details

3.1 Documentation and Evidence Reviewed

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

***Note**: When a reporting instruction asks to identify the evidence examined, the Secure SLC Assessor must identify the evidence (for example, as "Doc-1") in the table below and then specify the corresponding document reference number in the Assessor Response field next to the applicable reporting instruction in the Findings and Observations section. The assessor may add rows to this table as needed.*

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	

3.2 Individuals Interviewed

Identify and list the individuals interviewed during testing:

***Note**: When a reporting instruction asks to identify the individuals interviewed, the Secure SLC Assessor must identify the individuals (for example, as "Int-1") in the table below and then specify the corresponding interview reference number in the Assessor Response field next to the applicable reporting instruction in the Findings and Observations section. The assessor may add rows to this table as needed.*

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				

3.3 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 SLC 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 SLC 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 development personnel sampled in 1.3.b.			
Set-2	Software development personnel sampled in 2.2.b.			
Set-3	Software development personnel sampled in 2.3.b.			
Set-4	Security assurance processes sampled in 2.4.b.			
Set-5	Security assurance processes sampled in 2.5.b.			
Set-6	Security assurance processes sampled in 2.6.b.			
Set-7	Vendor payment software sampled in 3.2.c.			
Set-8	Vendor payment software sampled in 4.1.d.			
Set-9	Vendor software sampled in 4.2.b and 4.2.c.			

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-10	Changes sampled in 5.1.b.			
Set-11	Software updates sampled in 5.2.b.			
Set-12	Vendor systems sampled in 7.2.b.			
Set-13	Vendor software sampled in 8.1.b.			
Set-14	Software updates sampled in 8.3.b.			
Set-15	Software security updates sampled in 9.3.b.			
Set-16	Software updates sampled in 10.1.b.			

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, independent judgment and objectivity, disclosure, conflicts of interest, misrepresentations, and instruction of employees;
- This assessment was conducted in a manner intended to preserve at all times the professional judgment, integrity, impartiality and professional skepticism of the Assessor Company;
- This Report on Compliance 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 Compliance (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 Scoping Accuracy

- To the best of their knowledge, all information pertaining to the scope of this Secure SLC Assessment is accurately represented in “Section 2: Scope of the Secure SLC Assessment.”

4.3 Attestation of Sampling

- To the best of their knowledge, all sample sets used for this Secure SLC Assessment are accurately represented in “Section 3.3: 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

Control Objective 1: Security Responsibilities and Resources

The software vendor's senior leadership team establishes formal responsibility and authority for the security of the software vendor's products and services. The software vendor allocates resources to execute the strategy and to ensure that personnel are appropriately skilled.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
1.1 Overall responsibility for the security of the software vendor's products and services is assigned by the vendor's senior leadership team.			**In Place**	**N/A**	**Not in Place**
			□	□	□
1.1 The assessor shall examine vendor evidence and interview the individual or individuals assigned overall responsibility for the security of the vendor's products and services to confirm the following: • Accountability for ensuring the security of the software vendor's products and services is formally assigned to an individual or team by the software vendor's senior leadership. • Responsibilities include keeping senior leadership informed of security updates, issues, and other matters related to the security of the software vendor's products and services. • Updates are provided to senior leadership at least annually on the performance of and changes to the software vendor's software security policy and strategy described in Control Objective 2.	**Identify** the vendor evidence examined that confirms the findings for this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Identify the last date senior leadership were updated on issues or other matters related to the security of the software vendor's products and services, or changes to the software vendor's software security policy and/or strategy.				
	Describe the specific topics covered in that update.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
1.2 Software security responsibilities are assigned.			In Place	N/A	Not in Place
			☐	☐	☐
1.2.a The assessor shall examine vendor evidence to confirm the following: • Software security responsibilities are clearly defined and assigned to appropriate individuals or teams, including software development personnel. • Assignment of responsibilities for ensuring the security of the software vendor's products and services covers the entire software lifecycle.	**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 individuals or teams assigned responsibilities are appropriate for their given responsibilities.				
	Describe what the assessor observed in the vendor evidence to conclude that the software security responsibilities assigned to software vendor personnel cover the entire software lifecycle.				
1.2.b The assessor shall interview a sample of responsible individuals, including software development personnel, to confirm they are clearly aware of and understand their software security responsibilities.	**Identify** the responsible individuals interviewed that confirm responsible personnel are aware of and understand their software security responsibilities.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
1.3 Software development personnel maintain skills in software security matters relevant to their specific role, responsibility, and job function.			**In Place**	**N/A**	**Not in Place**
1.3.a The assessor shall examine vendor evidence to confirm the following: • A mature process is implemented and maintained for managing and maintaining software security skills for software development personnel. • The skills required for each defined role, responsibility, and job function are clearly defined. • The criteria for maintaining individual skills are clearly defined. • The process includes a review at least annually to ensure software development personnel are maintaining the necessary skills for the security responsibilities they have been assigned.	**Identify** the vendor evidence examined that confirms a process for ensuring software development personnel maintain their software security skills is implemented and maintained in a manner consistent with this test requirement.				
	Describe what the assessor observed in the vendor evidence to conclude that the software vendor's process for managing and maintaining personnel skills is mature (i.e., is established, repeatable across personnel and geographic locations, and whose output or outcomes are predictable).				
	Describe where the software vendor maintains the definitions of skills required for each role, responsibility and job function.				
	Summarize the software vendor's criteria for how software development personnel are expected to maintain their individual skills in software security matters relevant to their specific role, responsibility, and job function.				
	Describe what the assessor observed in the vendor evidence that demonstrates the software vendor performs reviews at least annually to ensure software development personnel are maintaining the necessary skills for the security responsibilities they have been assigned.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
1.3.b For a sample of software development personnel, examine vendor evidence and interview personnel to confirm the following: • Individuals have demonstrated that they possess the skills required for their role, responsibility, or job function. • Individuals have satisfied the criteria for maintaining their individual skills.	**Identify** the software development personnel sampled for this test requirement.		
	Identify the vendor evidence examined that confirms the findings for this test requirement.		
	For the sample of software development personnel, **describe** how the vendor evidence and interviews demonstrate that software development personnel: • Possess the skills required for their role, responsibility, and job function. • Have satisfied the vendor's criteria for maintaining their individual skills.		

Control Objective 2: Software Security Policy and Strategy

The software vendor defines, maintains, and communicates a software security policy and a strategy for ensuring the secure design, development, and management of its products and services. Performance against the software security strategy is monitored and tracked.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
2.1 Regulatory and industry security and compliance requirements applicable to the software vendor's operations, products, and services and the data stored, processed, or transmitted by the software vendor are identified and monitored.			In Place	N/A	Not in Place
			□	□	□
2.1 The assessor shall examine vendor evidence and interview personnel to confirm the following: • A mature process exists to identify and monitor external regulatory and industry security and compliance requirements. • The process includes reviewing sources of regulatory and industry security and compliance requirements for changes at least annually. • The process results in an inventory of external regulatory and industry security and compliance requirements. • The inventory is updated as external security and compliance requirements change.	**Identify** the vendor evidence examined that confirms a process is implemented in a manner consistent with this test requirement.				
	Identify the personnel interviewed confirm the findings for this test requirement.				
	Identify the date the external regulatory and industry security and compliance requirements were last reviewed to confirm that a review is performed at least annually.				
	Describe where the software vendor maintains the inventory of external regulatory and industry security and compliance requirements.				
	Describe what the assessor observed in the vendor evidence that demonstrates the inventory is updated when external security and compliance requirements change.				
			In Place	N/A	Not in Place

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)		
2.2 A software security policy is defined and establishes the specific rules and goals for ensuring the software vendor’s products and services are designed, developed, and maintained to be secure, resistant to attack, and in a manner that satisfies the software vendor’s security and compliance obligations.			□	□	□
2.2.a The assessor shall examine vendor evidence to confirm the following: • A software security policy exists and is communicated to appropriate software vendor personnel and business partners, including all software development personnel. • At a minimum, the policy covers all control objectives within this standard (either explicitly or implicitly). • The policy is defined in sufficient detail such that the security rules and goals are measurable. • The software vendor’s senior leadership team has approved the software security policy.	**Identify** the vendor evidence examined that confirms a software security policy is defined and maintained in a manner consistent with this test requirement.				
	Describe what the assessor observed in the vendor evidence that confirms each control objective within this standard is covered in the software vendor’s software security policy.				
	Describe what the assessor observed in the vendor evidence to conclude that the policy is defined in sufficient detail such that the security rules and goals within the policy are measurable.				
	Describe what the assessor observed in the vendor evidence to conclude the software vendor’s senior leadership have approved the software security policy.				
2.2.b The assessor shall interview a sample of software development personnel to confirm they are aware of and understand the software security policy.	**Identify** the software development personnel sampled for this test requirement.				
	Describe what was discussed during the interviews that led the assessor to conclude the personnel interviewed are aware of and understand the software security policy.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
2.3 A formal software security strategy for ensuring the security of the software vendor's products and services and satisfying its software security policy is established and maintained.			In Place	N/A	Not in Place
			□	□	□
2.3.a The assessor shall examine vendor evidence and interview responsible personnel to confirm the following: • A strategy for ensuring the security of the software vendor's products and services is defined. • The software security strategy clearly outlines how the software security policy is to be satisfied. • The software security strategy is based on or aligned with industry-accepted methodologies. • The software security strategy covers the entire lifecycle of the software vendor's software products and services. • The software security strategy is communicated to appropriate personnel, including software development personnel. • The software security strategy is reviewed at least annually and updated as needed (such as when business needs, external drivers, and products and services evolve).	**Identify** the vendor evidence examined that confirms a strategy for ensuring the security of the software vendor's products and services is defined and maintained in a manner consistent with this test requirement.				
	Identify the responsible personnel interviewed that confirm the findings for this test requirement.				
	Identify the industry-accepted methodologies upon which the software vendor's software security strategy is based or with which it aligns.				
	Describe what the assessor observed in the vendor evidence to conclude that the software security strategy covers the entire software lifecycle for the software vendor's products and services.				
	Identify the date upon which the software security strategy was last reviewed to confirm that a review is performed at least annually.				
	Describe what the assessor observed in the vendor evidence and discovered through interviews to conclude that the software security strategy is updated when factors such as business needs, external drivers, and products and services evolve.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
2.3.b The assessor shall interview a sample of software development personnel to confirm they are aware of and understand the software security strategy.	**Identify** the software development personnel sampled for this test requirement.				
	Describe what was discussed during the interviews that led the assessor to conclude the software development personnel interviewed are aware of and understand the software security strategy.				
2.4 Software security assurance processes are implemented and maintained throughout the entire software lifecycle.			**In Place**	**N/A**	**Not in Place**
Note*: This control objective focuses on the overall management of security assurance processes and provides the foundation for specific assurance processes defined within this document.*			□	□	□
2.4.a The assessor shall examine vendor evidence and interview personnel to confirm the following: • Software security assurance processes are defined, implemented and maintained. • An inventory of software security assurance processes is maintained.	**Identify** the vendor evidence examined that confirms software security assurance processes are defined and maintained in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Describe where the software vendor maintains the inventory of software security assurance processes.				
2.4.b For a sample of software security assurance processes, the assessor shall	**Identify** the software security assurance processes sampled for this test requirement.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
examine vendor evidence and interview personnel to confirm the following: • Software security assurance processes clearly address the specific rules and goals within the software vendor's software security policy. • Software security assurance processes are aligned with the software vendor's software security strategy. • Software vendor personnel, including software development personnel, are assigned responsibility and accountability for the execution and performance of the security assurance process in accordance with Control Objective 1.2. • The individuals or teams responsible for performing and maintaining each security assurance process are clearly aware of their responsibilities. • The results or outcomes of each security assurance process are monitored in accordance with Control Objective 2.6.	For the software security assurance processes sampled, **identify** the evidence examined that confirms that software security assurance processes are defined and implemented in a manner consistent with this test requirement.		
	For the software security assurance processes selected, **describe** what the assessor observed in the vendor evidence and discovered through interviews to conclude the processes are aligned with the software vendor's software security strategy.		
	Identify the responsible individuals interviewed that confirm they are clearly aware of their responsibilities.		
	For the software security assurance processes sampled, **describe** how the vendor evidence demonstrates that the results or outcomes of the software security assurance processes are monitored in accordance with Control Objective 2.6.		

2.5 Evidence is generated and maintained to demonstrate the effectiveness of software security assurance processes.	**In Place**	**N/A**	**Not in Place**
	□	□	□

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
2.5.a The assessor shall examine vendor evidence, including the inventory of software security assurance processes described in Test Requirement 2.4.a, and interview personnel to confirm that evidence is generated and maintained for each security assurance process.	**Identify** the vendor evidence examined that confirms that the security assurance processes generate evidence that demonstrates their effectiveness.				
	Identify the individuals interviewed that confirms the findings for this test requirement.				
2.5.b For a sample of security assurance processes, the assessor shall examine evidence and other output from the processes and interview personnel to confirm the evidence generated for each process reasonably demonstrates the process is operating effectively and as intended.	**Identify** the security assurance processes sampled for this test requirement.				
	Identify the evidence examined that confirms the findings for this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	For each of the security assurance processes sampled, **describe** the location(s) where evidence of the processes' effectiveness is generated and stored.				
	For each of the security assurance processes sampled, **describe** what the assessor observed in the vendor evidence to conclude that the evidence generated by each process is reasonable (i.e., appropriate) for demonstrating the effectiveness of the process.				
2.6 Failures or weaknesses in software security assurance processes are detected. Weak or ineffective security assurance processes are updated, augmented or replaced.			**In Place**	**N/A**	**Not in Place**
			□	□	□

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
2.6.a The assessor shall examine vendor evidence and interview personnel to confirm the following: • A mature process exists to detect and evaluate weak or ineffective security assurance processes. • The criteria for determining a weak or ineffective security assurance process is defined and justified. • Security assurance processes are updated, augmented or replaced when deemed weak or ineffective.	**Identify** the vendor evidence examined that confirms a process is implemented in a manner consistent with this test requirement.		
	Identify the individuals interviewed that validate the findings for this test requirement.		
	Describe where the software vendor maintains its criteria and justifications for how it defines weak or ineffective security assurance processes.		
	Describe what the assessor observed in vendor evidence and discovered through interviews to conclude that security assurance processes are updated, augmented or replaced when deemed weak or ineffective.		
2.6.b For a sample of the security assurance processes identified in Control Objective 2.4, the assessor shall interview personnel and examine any additional evidence necessary to determine if any failures or weaknesses in those security processes occurred, and to confirm that weak or ineffective processes were updated, augmented or replaced. *(continued on next page)*	**Identify** the security assurance processes sampled for this test requirement.		
	Identify the evidence examined that confirms the findings for this test requirement.		
	Identify the individuals interviewed that confirm the findings for this test requirement.		
	Describe how the assessor determined whether any failures or weaknesses in the implemented security assurance processes occurred.		
	For the security assurance processes sampled, **indicate** whether any failures or		

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
	weaknesses have occurred within the last year (yes/no). *If "no," skip to 3.1. If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the vendor evidence to conclude that the weak or ineffective security assurance processes were updated, augmented or replaced.		

Control Objective 3: Threat Identification and Mitigation

The software vendor continuously identifies, assesses, and manages risk to its software and services.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)		
3.1 Critical assets are identified and classified.			**In Place**	**N/A**	**Not in Place**
			□	□	□
3.1 The assessor shall examine vendor evidence to confirm the following: • A mature process exists to identify and classify critical assets. • The criteria for identifying critical assets and determining the confidentiality, integrity, and resiliency requirements for each critical asset are defined. • The process accounts for all types of critical assets—including sensitive data, sensitive resources, and sensitive functions—for the vendor’s software. • The process results in an inventory of critical assets used by the vendor’s software.	**Identify** the vendor evidence examined that confirms a process is implemented to identify and classify critical assets in a manner that is consistent with this test requirement.				
	Summarize the software vendor’s process for determining critical assets in the vendor’s software.				
	Describe what the assessor observed in the vendor evidence to conclude that the implemented process accounts for all types of critical assets, including the sensitive data, sensitive functions and sensitive resources provided or used by the vendor’s software.				
	Describe where the software vendor maintains the inventory of critical assets used by the vendor’s software.				
3.2 Threats to software and weaknesses within its design are continuously identified and assessed.			**In Place**	**N/A**	**Not in Place**

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
			□	□	□
3.2.a The assessor shall examine vendor evidence, including process documentation and assessment results to confirm the following: • A mature process exists to identify, assess, and monitor software threats and design weaknesses (i.e., flaws). • The assessment accounts for all software inputs/outputs, process/data flows, trust boundaries and decision points, and how they may be exploited by an attacker. • The assessment accounts for the entire code base, including how the use of third-party, open-source, or shared components or libraries, APIs, services, and applications used for the delivery and operation of the software may be leveraged in an attack. • The assessment results in a recorded inventory of threats and design flaws. • Assessments are routinely performed to account for changes to existing or the emergence of new threats or design flaws.	**Identify** the vendor evidence examined that confirms a process is implemented to identify, assess, and monitor software threats and design weaknesses in a manner that is consistent with this test requirement.				
	Explain the assessor's rationale for concluding the implemented process is mature.				
	Describe what the assessor observed in the vendor evidence to conclude the software vendor's process accounts for all software inputs and outputs, process/data flows, and trust boundaries and decision points, and how they may be exploited by an attacker.				
	Describe how the vendor evidence demonstrates that the assessment accounts for the entire code base, including the use of third-party, open-source or shared components or libraries, APIs, services, and applications used for the delivery and operation of the software.				
	Describe how and where the software vendor maintains threat and design flaw assessment results.				
	Describe the frequency and additional triggers that cause threat and design flaw assessments to be initiated.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)
3.2.b Where open-source software components are utilized as part of the software, the assessor shall examine vendor evidence, including process documentation and assessment results to confirm these components are managed as follows: • An inventory of open-source components used in the vendor’s software is maintained. • A mature process exists to analyze and mitigate the use of open-source components with known vulnerabilities. • The software vendor monitors vulnerabilities in open-source components throughout their use or inclusion in the vendor’s software. • An appropriate patching strategy for open-source components is defined.	**Describe** how the assessor determined whether the software vendor utilizes open-source components in their software.		
	Indicate whether the software vendor utilizes open-source software components in their software (yes/no). *If “no,” skip to 3.2.c. If “yes,” complete the remaining reporting instructions for this test requirement.*		
	Identify the vendor evidence examined that confirms a process is implemented to manage open-source software components in a manner consistent with this test requirement.		
	Describe how and where the software vendor maintains an inventory of open-source components used in the vendor’s software.		
	Describe what the assessor observed in the vendor evidence to conclude that a mature process is implemented to analyze and mitigate the risks posed by the use of known-vulnerable open-source components.		
	Summarize how the software vendor monitors vulnerabilities in open-source components throughout their use or inclusion in the vendor’s software.		
	Describe how the assessor arrived at the conclusion that the software vendor’s patching strategy for open-source components is appropriate.		

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
3.2.c For a sample of vendor software, the assessor shall examine assessment results for the selected software to confirm the following: • All software inputs/outputs, process/data flows, trust boundaries and decision points were considered during the assessment. • The entire code base, including how the use of third-party, open-source or shared components or libraries, APIs, services, and applications used for the delivery and operation of the software were considered during the assessment.	**Identify** the vendor software sampled for this test requirement.		
	For the vendor software sampled, **identify** the date(s) of the most recent assessment of software threats and design weaknesses to confirm assessments are performed.		
	For the vendor software sampled, **describe** what the assessor observed in the assessment results to conclude that the following were considered during the assessment: • All software inputs/outputs. • All process/data flows. • All trust boundaries. • All decision points.		
	For the vendor software sampled, **describe** what the assessor observed in the assessment results to conclude that the entire code base was considered during the assessment, including: • The use of all third-party, open-source, or shared components and libraries. • All APIs, services and applications used for the delivery and operation of the software.		

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)		
3.3 Software security controls are implemented in the software to mitigate threats and design weaknesses.			**In Place**	**N/A**	**Not in Place**
			□	□	□
3.3.a The assessor shall examine vendor evidence, including process documentation and software-specific threat and design information, to confirm the following: • A mature process exists for defining software-specific security requirements and implementing software security controls within the software to mitigate software threats and design flaws. • Decisions on whether and how to mitigate a specific threat or design flaw are recorded, justified, and approved by appropriate personnel. • Any remaining residual risk is recorded, justified, and approved by appropriate personnel.	**Identify** the vendor evidence examined that confirms a process is implemented for defining software-specific security requirements and implementing software security controls within the software vendor’s software in a manner consistent with this test requirement.				
	Describe how the vendor evidence examined demonstrates that decisions on whether and how to mitigate a specific threat or design flaw are recorded, justified, and approved by appropriate software vendor personnel.				
	Describe what the assessor observed in the vendor evidence to conclude that residual risk is also recorded, justified and approved by appropriate personnel.				
3.3.b The assessor shall examine evidence and interview personnel to confirm the following: • Decisions on whether and how to mitigate a specific threat or design flaw are reasonably justified. • Any remaining residual risk is reasonably justified.	**Identify** the vendor evidence examined that confirms the findings for this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				

Control Objectives 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 discovered through interviews to conclude that justifications for the following are considered reasonable: • Decisions on whether and how to mitigate threats and design flaws. • Any remaining residual risk.				
3.3.c The assessor shall examine vendor evidence to confirm that security controls have been implemented to mitigate all identified threats and design flaws.	**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 security controls are implemented to mitigate identified threats and design flaws.				
3.4 Failures or weaknesses in software security controls are detected. Weak or ineffective security controls are updated, augmented or replaced.			**In Place**	**N/A**	**Not in Place**
			□	□	□
3.4.a The assessor shall examine vendor evidence and interview personnel to confirm the following: • A mature process exists to identify weak or ineffective software security controls and to update, augment, or replace them. • The criteria for determining a weak or ineffective security control is defined and justified. • The process involves monitoring security control effectiveness throughout the software lifecycle. *(continued on next page)*	**Identify** the vendor evidence examined that confirms a process is implemented to identify and update weak or ineffective software security controls in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Describe where the software vendor defines and maintains effectiveness criteria for software security controls.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)
• Weak or ineffective security controls are updated, augmented, or replaced in a timely manner upon detection.	**Describe** what the assessor observed in the vendor evidence and discovered through interviews to conclude software security control effectiveness is monitored throughout the software lifecycle.		
	Describe how the assessor determined that, upon detection of weak or ineffective software security controls, the software security controls are updated, augmented or replaced in an timely manner.		
3.4.b The assessor shall examine vendor evidence, including software-specific data or test results, and details of software-specific updates to confirm the following: • Security controls that have been deemed “weak” or “ineffective” have been updated, augmented or replaced. • Decisions on whether and how to replace and augment weak or ineffective security controls are made in accordance with defined criteria and with Control Objective 3.3.	**Identify** the vendor evidence examined that confirms the findings for this test requirement.		
	Indicate whether the evidence examined shows that weak or ineffective software security controls were detected by the vendor (yes/no). *If “no,” skip to 4.1. If “yes,” complete the remaining reporting instructions for this test requirement.*		
	Where weak or ineffective security controls were detected, **describe** what the assessor observed in the vendor evidence to conclude that the weak or ineffective security controls have been updated, augmented or replaced.		
	Describe how the vendor evidence demonstrates that decisions on how to mitigate the weak or ineffective security controls were made in accordance with the defined criteria and with Control Objective 3.3.		

Control Objective 4: Vulnerability Detection and Mitigation

The software vendor detects and mitigates vulnerabilities in software to ensure that its software remains resistant to attacks throughout its entire lifecycle.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
4.1 Existing and emerging software vulnerabilities are detected in a timely manner.			**In Place**	**N/A**	**Not in Place**
			□	□	□
4.1.a The assessor shall examine vendor evidence and interview personnel to confirm the following: • A mature process exists for testing software for the existence and emergence of vulnerabilities (i.e., security testing). • Tools or methods used for security testing are appropriate for detecting applicable vulnerabilities in the vendor's software, and are suitable for the software architectures, and the software development languages and frameworks employed. • Security testing is performed throughout the entire software lifecycle, including after release. • Security testing accounts for the entire code base, including detecting vulnerabilities in any third-party, open-source, and shared components and libraries. • Security testing is performed by authorized and objective vendor personnel or third parties. *(continued on next page*	**Identify** the vendor evidence examined that confirms a process for testing software for the existence and emergence of vulnerabilities is implemented in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Summarize how the software vendor defines the tools and methods used for testing the vendor's software for vulnerabilities.				
	Describe what the assessor observed in the vendor evidence to conclude that security testing is performed throughout the software lifecycle, including after release.				
	Describe how the vendor evidence demonstrates that security testing accounts for the entire code base, including accounting for vulnerabilities in third-party, open-source and shared components and libraries.				
	Describe how the software vendor's process ensures that security testing is				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
• Security testing results in an inventory of identified vulnerabilities. • Security-testing details including the tools used, their configurations, and the specific tests performed are recorded and retained.	only performed by authorized and objective vendor personnel or third-parties.		
	Describe where the software vendor maintains the inventory of identified vulnerabilities for the vendor's software and software components.		
	Describe how and where security-testing details, including the tools used, their configurations, and the specific tests performed are recorded and retained.		
4.1.b The assessor shall examine evidence, including software-specific security testing configurations and test results to confirm the following: • Security-testing tools are configured in a manner that is appropriate for the intended tests performed. • Security testing accounts for the entire code base, including detecting vulnerabilities in any third-party, open-source, and shared components and libraries. • Security testing was performed by authorized and objective vendor personnel or third parties.	**Identify** the evidence examined that confirms the findings for this test requirement.		
	Describe how the assessor determined that the security-testing tools used for software-specific security testing were configured in a manner appropriate for the tests they were intended to perform.		
	Describe what the assessor observed in the vendor evidence to conclude that the testing accounted for entire code base, including third-party, open-source, or shared components and libraries.		
	Describe how the assessor determined that security testing was performed by authorized and objective software vendor personnel or third-parties.		
4.1.c The assessor shall examine vendor evidence and interview personnel to confirm that personnel responsible for testing are knowledgeable and skilled in	**Identify** the vendor evidence examined that confirms the findings for this test requirement.		

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
the following areas in accordance with Control Objective 1.3: - Software security testing techniques - Security testing tools settings, configurations, and recommended usage	**Identify** the individuals interviewed that confirm the findings for this test requirement.				
	Describe what the assessor observed in the vendor evidence and discovered through interviews that led the assessor to conclude that personnel responsible for the security testing are knowledgeable and skilled in the areas of: - Software security testing techniques - Security testing tools settings, configurations, and recommended usage				
4.1.d For a sample of vendor software, examine software-specific testing results to confirm that security testing is performed throughout the software lifecycle.	**Identify** the vendor software sampled for this test requirement.				
	Identify the vendor evidence examined that confirms the findings for this test requirement.				
	For the sampled software, **describe** what the assessor observed in the vendor evidence to conclude that security testing is performed throughout the software lifecycle.				
4.2 Newly discovered vulnerabilities are fixed in a timely manner. The reintroduction of similar or previously resolved vulnerabilities is prevented.			**In Place**	**N/A**	**Not in Place**
			□	□	□

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)
4.2.a The assessor shall examine vendor evidence and interview personnel to confirm the following: • A mature process exists for distributing and deploying fixes for newly discovered vulnerabilities and preventing the reintroduction of previously resolved vulnerabilities. • The process includes methods to prevent previously resolved vulnerabilities or other similar vulnerabilities from being reintroduced into the software. • The criteria for determining the “criticality” or “severity” of vulnerabilities and how to address vulnerabilities are defined and justified. • Fixes to address vulnerabilities in production code are made available and deployed in accordance with defined criteria. • Decisions not to provide fixes in accordance with defined criteria are approved and justified by appropriate personnel on a case-by-case basis.	**Identify** the vendor evidence examined that confirms a process for distributing and deploying fixes for newly discovered vulnerabilities and preventing the reintroduction of previously resolved vulnerabilities is implemented in a manner consistent with this test requirement.		
	Identify the personnel interviewed that confirm the findings for this test requirement.		
	Summarize how the software vendor prevents previously resolved vulnerabilities or similar vulnerabilities from being reintroduced into software.		
	Describe where the software vendor’s criteria for determining the criticality or severity of vulnerabilities and how to address them are defined and justified.		
	Summarize how fixes to address vulnerabilities in production code are made available and deployed in accordance with defined critieria.		
	Describe what the assessor observed in the vendor evidence and discovered through interviews to conclude that decisions not to provide fixes in accordance with defined criteria are approved and justified by appropriate personnel on a case-by-case basis.		
4.2.b For a sample of vendor software, the assessor shall examine software-	**Identify** the vendor software sampled for this test requirement.		

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
specific security-testing results and the details of software updates to confirm that security fixes are made available and deployed (where applicable) in accordance with defined criteria.	**Identify** the evidence examined that confirms the findings for this test requirement.		
	For the sampled software, **describe** what the assessor observed in the vendor evidence to conclude that security fixes are made available and deployed in accordance with defined criteria.		
4.2.c For a sample of vendor software, the assessor shall interview personnel to confirm that decisions not to provide security fixes in accordance with defined criteria are justified by appropriate personnel.	For the sampled software, **indicate** whether any decisions to not provide security fixes in accordance with defined criteria were identified (yes/no). *If "no," skip to 5.1. If "yes," complete the remaining reporting instructions for this test requirement.*		
	For the sampled software, **identify** the vulnerabilities for which a decision was made not to provide a fix in accordance with the vendor's defined criteria.		
	For the sampled software and vulnerabilities for which a decision was made not to provide a security fix in accordance with the vendor's defined criteria, **describe** how the assessor arrived at the conclusion that the software vendor's justification for not providing a fix is reasonable.		
	Identify the individuals interviewed who confirm the findings for this test requirement.		

Control Objective 5: Change Management

The software vendor identifies and manages all software changes throughout the software lifecycle.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
5.1 All changes to software are identified, assessed, and approved.			In Place	N/A	Not in Place
			□	□	□
5.1.a The assessor shall examine vendor evidence and interview personnel to confirm: • A mature process exists to identify, assess, and approve all changes to software. • The process includes an analysis of the security impact of all changes. • The process results in an inventory of all changes made to software, including a record of the determined security impact. • All change-management decisions are recorded. • All implemented changes are authorized by responsible personnel. • The inventory of changes identifies the individual creator of the code and individual authorizing the change, for each code change. • All decisions to implement changes are justified.	**Identify** the vendor evidence examined that confirms a process is implemented in a manner that is consistent with this test requirement.				
	Identify the individuals interviewed who confirm the findings for this test requirement.				
	Summarize how security impact is considered as part of the process to identify, assess, and approve all changes to software.				
	Describe where the software vendor maintains its inventory of all software changes.				
	Describe where all change management decisions are recorded.				
	Summarize how the software vendor ensures that all implemented changes are authorized by responsible personnel.				
	Summarize how the software vendor ensures that the code creator and individual authorizing the change are accurately recorded in the inventory of changes.				
	Describe how the vendor evidence demonstrates that all implemented changes are justified.				
5.1.b For a sample of changes, the assessor shall examine software-specific	**Identify** the changes sampled for this test requirement.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
and change-specific documentation or evidence to confirm the following: • All changes are authorized by responsible personnel. • All decisions to implement the changes are recorded and include justification for the change. • The inventory of changes clearly identifies the individual creator of the code and the individual authorizing the change, for each code change.	**Identify** the evidence examined that confirms the findings for this test requirement.				
5.2 All software versions are uniquely identified and tracked throughout the software lifecycle.			In Place	N/A	Not in Place
			□	□	□
5.2.a The assessor shall examine vendor evidence and interview personnel to confirm the following: • A formal system or methodology for uniquely identifying each version of software is defined. • The system or methodology includes arranging unique identifiers or version elements in a sequential and logical manner. • All changes to software functionality are clearly associated with a unique software version.	**Identify** the vendor evidence examined that confirms the findings for this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Summarize the software vendor's methodology for uniquely identifying its software, including how the software vendor arranges identifiers or version elements in a sequential and logical manner.				
	Describe what the assessor observed in vendor evidence and discovered through interviews to conclude that all changes to software functionality are associated with a unique software version.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
5.2.b For a sample of software updates, the assessor shall examine vendor evidence, including change-specific documentation, to confirm the following: • Software versions are updated in accordance with the defined versioning system or methodology. • All changes to software functionality are clearly associated with a unique software version.	**Identify** the software updates sampled for this test requirement.		
	Identify the vendor evidence examined that confirms the findings for this test requirement.		
	For the sample of software updates, **describe** what the assessor observed in the vendor evidence to conclude that software versions are updated and maintained in a manner consistent with the defined system or methodology.		

Control Objective 6: Software Integrity Protection

The integrity of software is protected through the software lifecycle.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
6.1 The integrity of all software code, including third-party components, is maintained throughout the entire software lifecycle.			**In Place**	**N/A**	**Not in Place**
			□	□	□
6.1 The assessor shall examine evidence, interview personnel, and observe tools and processes to confirm: • A mature process, mechanism, and/or tool(s) exist to protect the integrity of the software code, including third-party components. • The processes, mechanisms, and/or tools are reasonable and appropriate for protecting the integrity of software code. • Processes, mechanisms, or the use of tools results in the timely detection of any unauthorized attempts to tamper with or access software code. • Unauthorized attempts to tamper with or access software code are investigated in a timely manner.	**Identify** the vendor evidence examined that confirms that a process, mechanism and/or tools to protect the integrity of software code are implemented in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirms the findings for this test requirement.				
	Summarize how the software vendor protects the integrity of its software code.				
	Describe how the assessor arrived at the conclusion that the implemented processes, mechanisms, and/or tools for protecting the integrity of the code are reasonable and appropriate (i.e., fit-for-purpose).				
	Describe what the assessor observed in the vendor evidence and discovered through interviews to conclude that unauthorized attempts to tamper with or access software code are detected and investigated in a timely manner.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
6.2 Software releases and updates are delivered in a secure manner that ensures the integrity of the updated code.			**In Place**	**N/A**	**Not in Place**
			□	□	□
6.2 The assessor shall examine vendor evidence, interview personnel, and observe tools and processes to confirm the following: • A mature process, mechanism, and/or tool(s) exist to ensure the integrity of software updates during delivery. • The processes, mechanisms, and/or tools are reasonable and appropriate for protecting the update code. • Processes, mechanisms, and/or the use of tools results in the secure delivery of updated code.	**Identify** the vendor evidence examined that confirms processes, mechanisms and/or tool(s) to ensure the integrity of software updates during delivery are implemented in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Describe the processes, mechanisms, and/or tools used by the vendor to ensure the integrity of software updates during delivery.				
	Describe what the assessor observed in the vendor evidence and discovered through interviews to conclude that the implemented processes, mechanisms and/or tool(s) are reasonable and appropriate for protecting the updated code.				
	Describe how the assessor determined that the implemented processes, mechanisms and/or tool(s) result in the secure delivery of updated code.				

Control Objective 7: Sensitive Data Protection

The confidentiality of sensitive production data is maintained on vendor systems.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
7.1 Sensitive productiondata is only collected and retained on software vendor systems where there is a legitimate business or technical need.			**In Place**	**N/A**	**Not in Place**
			□	□	□
7.1. The assessor shall examine vendor evidence and interview personnel to confirm the following: • A mature process exists to record and authorize the collection and retention of any sensitive production data. • An inventory of sensitive production data captured or stored by the software vendor's products and services is maintained. • Decisions to use sensitive production data are approved by appropriate software vendor personnel. • Decisions to use sensitive production data are recorded and reasonably justified.	**Identify** the vendor evidence examined that confirms a process to record and authorize the collection and retention of any sensitive production data is implemented in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Identify the location where the software vendor maintains an inventory of sensitive production data captured or stored by the software vendor's products or services.				
	Describe what the assessor observed in the vendor evidence and discovered through interviews to conclude that the software vendor's use of sensitive production data is approved by appropriate software vendor personnel.				
	Describe where software vendor decisions to use sensitive production data are recorded.				
	Describe how the assessor arrived at the conclusion that the software vendor's justifications for using sensitive production data are reasonable.				
			In Place	**N/A**	**Not in Place**

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)		
7.2 Sensitive production data is protected when retained on software vendor systems and securely deleted when no longer needed.			□	□	□
7.2.a The assessor shall examine vendor evidence and interview personnel to confirm that a mature process exists to ensure sensitive production data is protected when retained on software vendor systems and is securely deleted when no longer needed.	**Identify** the vendor evidence examined that confirms a mature process is implemented to ensure sensitive production data is protected when retained on software vendor systems and securely deleted when no longer needed.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Summarize how the software vendor ensures sensitive production data is protected when retained on vendor systems.				
	Describe the tools and/or methods used by the software vendor to securely delete sensitive production data (i.e., render irretrievable) when no longer needed.				
7.2.b The assessor shall examine vendor evidence and observe a sample of vendor systems to confirm the following: • Sensitive production data is not resident on software vendor systems unless appropriate evidence of approval and justification exists. • Sensitive production data is appropriately protected where it is retained. *(continued on next page)*	**Identify** the vendor systems sampled for this test requirement.				
	Identify the vendor evidence examined that confirms the findings for this test requirement.				
	Describe how vendor systems were tested to determine whether sensitive production data is resident on those systems.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
• Secure deletion processes or mechanisms are sufficient to render sensitive production data irretrievable.	**Indicate** whether sensitive production data was observed to be resident on the sampled vendor systems (yes/no). *If "no," skip to 8.1. If "yes," complete the remaining reporting instructions for this test requirement.*		
	Describe what the assessor observed in the vendor evidence and on the sampled systems to conclude that all retention of sensitive production data on software vendor systems is justified and approved.		
	Describe how the assessor arrived at the conclusion that the sensitive production data is appropriately protected where it is retained.		
	Describe how the assessor confirmed that the secure deletion processes or mechanisms are sufficient to render the sensitive production data irretrievable.		

Control Objective 8: Software Vendor Implementation Guidance

The software vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of its software.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
8.1 The software vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of its software.			**In Place**	**N/A**	**Not in Place**
			□	□	□
8.1.a The assessor shall examine vendor evidence and interview personnel to confirm the following: • A mature process exists to produce, maintain, and make available to stakeholders guidance on the secure implementation, configuration, and operation of its software. • The implementation guidance includes documentation of all configurable security-related options and parameters for the vendor's software, and instructions for properly configuring and securing each of those options and parameters.	**Identify** the vendor evidence examined that confirms a process to produce, maintain, and make available to stakeholders guidance on the secure implementation, configuration, and operation of its software is implemented in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Summarize how the software vendor makes guidance on the proper configuration of all security-related options and parameters in the vendor's software available to stakeholders.				
8.1.b For a sample of vendor software, examine software-specific documentation and materials to confirm that the software vendor provides and maintains guidance on the secure configuration of each security-related option or parameter available in the vendor's software.	**Identify** the vendor software sampled for this test requirement.				
	Identify the software-specific documentation and materials examined that detail all of the configurable security-related options and parameters available for the sampled software.				
	For the sample of vendor software, **describe** what was observed in the				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
	software-specific documentation and materials that led the assessor to conclude that the software vendor provides guidance on the secure configuration of all security-related options and parameters available in the sampled software.				
8.2 Secure implementation guidance includes detailed instructions on how to securely install, configure, and maintain all software components and supported platforms.			**In Place**	**N/A**	**Not in Place**
			□	□	□
8.2 The assessor shall examine vendor evidence, to confirm the following: • The secure implementation guidance includes instructions on how to securely install or initialize, configure, and maintain the software. • The secure implementation guidance is sufficiently detailed. • Evidence exists or is obtained to illustrate that following the secure implementation guidance results in a secure software configuration.	**Identify** the vendor evidence examined that confirms the findings for this test requirement.				
	Describe the rationale used by the assessor to determine whether the software vendor's secure implementation guidance is sufficiently detailed for stakeholders.				
	Describe what the assessor observed in the vendor evidence to conclude that following the secure implementation guidance results in a secure software configuration.				
8.3 Secure implementation guidance is aligned with software updates.			**In Place**	**N/A**	**Not in Place**
			□	□	□
8.3.a The assessor shall examine vendor evidence and interview personnel to confirm the following: *(continued on next page)*	**Identify** the vendor evidence examined that confirms a process is implemented in a manner consistent with this test requirement.				
• The process to produce and maintain secure implementation guidance includes generation of updated guidance when new	**Identify** the individuals interviewed that confirm the findings for this test requirement.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)
software updates are released, or security-related options or parameters are introduced or modified. • Secure implementation guidance is reviewed at least annually for accuracy even if updates to security-related options and parameters are not issued.	**Identify** the date of the last secure implementation guidance review to confirm a review is performed at least annually.		
	Describe what the assessor observed in the vendor evidence or discovered through interviews to conclude that secure implementation guidance is reviewed even if updates to security-related options and parameters are not issued.		
8.3.b For a sample of software updates, examine secure implementation guidance as well as details of the software updates to confirm that as security-related options and parameters are updated or added, the secure implementation guidance is updated.	**Identify** the software updates sampled for this test requirement that included updates to security-related options and parameters.		
	Identify any other vendor evidence or details of the software updates examined (such as release notes, etc.) that confirm the findings for this test requirement.		
	For the software updates sampled, **describe** what the assessor observed in the secure implementation guidance and details of the software updates to conclude that security guidance was updated when security-related options and parameters were updated or added.		

Control Objective 9: Stakeholder Communications

The software vendor maintains communication channels with stakeholders regarding potential security issues and mitigation options.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
9.1 Communication channels are defined and made available for customers, installers, integrators, and other relevant parties to report and receive information on security issues and mitigation options.			In Place	N/A	Not in Place
			□	□	□
9.1 The assessor shall examine evidence and interview personnel to confirm the following: • A mature process exists to support open, bi-directional communications with stakeholders for reporting and receiving security information regarding the software vendor's products and services. • Communication channels provide stakeholders the ability to report security-related issues and to receive timely status updates on their queries. • The software vendor maintains resources to respond to reports or inquiries regarding the security of the vendor's products and services.	**Identify** the vendor evidence examined that confirms a process to support open, bi-directional communications with stakeholders for reporting and receiving security information regarding the software vendor's products and services is implemented in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Summarize how the software vendor enables stakeholders to report and receive information on security issues and mitigation options in relation to the software vendor's products and services.				
	Summarize how the software vendor maintains resources to respond to reports and inquiries regarding the security of the software vendor's products and services.				
9.2 Stakeholders are notified about security updates in a timely manner.			In Place	N/A	Not in Place
			□	□	□
9.2 The assessor shall examine evidence and interview personnel to confirm a mature process exists to notify stakeholders about security updates in a timely manner.	**Identify** the vendor evidence examined that confirms a process is implemented to notify stakeholders about security updates in a timely manner.				
	Identify the individuals interviewed that confirms the findings for this test requirement.				

Control Objectives 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 discovered through interviews to conclude that stakeholders are notified about security updates in a timely manner.				
9.3 Where security updates are not readily available to address known vulnerabilities or exploits, security notifications are issued to all relevant stakeholders to provide instructions for mitigating the risks associated with the known vulnerabilities and exploits.			**In Place**	**N/A**	**Not in Place**
			□	□	□
9.3.a The assessor shall examine evidence and interview personnel to confirm that processes include providing stakeholders with instructions for mitigating the threat, or reducing the likelihood and/or impact of exploitation of known security issues for which a timely patch is not provided.	**Identify** the vendor evidence examined that confirms the findings for this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Summarize how the software vendor ensures risk mitigation instructions are provided to stakeholders for known vulnerabilities and exploits for which a timely patch is not provided.				
9.3.b For a sample of software security updates, examine stakeholder communications, product-specific documentation, security-testing results, or other materials to confirm that where known vulnerabilities are not addressed in the security updates, risk mitigation instructions are provided to stakeholders.	**Identify** the software security updates sampled for this test requirement where known vulnerabilities were not addressed in the update.				
	Identify the stakeholder communications, product-specific documentation, security-testing results, or other materials examined that confirm the findings for this test requirement.				
	For each of the software security updates sampled**, describe** what the assessor observed in the stakeholder communciations, product-specific				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)
	documentation, security-testing results, or other materials that confirm that stakeholders are provided risk mitigation instructions when a patch to address a known vulnerability not readily available.		

Control Objective 10: Software Update Information

The software vendor provides stakeholders with detailed explanations of all software changes.

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)		
10.1 Upon release of any software updates, a summary of the specific changes made to the software is provided to stakeholders.			**In Place**	**N/A**	**Not in Place**
			□	□	□
10.1.a The assessor shall examine evidence and interview personnel to confirm the following: • A mature process exists to communicate all software changes to stakeholders upon software updates. • The process results in a clear and detailed summary of all software changes. • The change summary information clearly outlines the specific software functionality impacted by the changes. • Change details are easily accessible to stakeholders.	**Identify** the evidence examined that confirms a process to communicate all software changes to stakeholders upon software updates is implemented in a manner consistent with this test requirement.				
	Identify the individuals interviewed that confirm the findings for this test requirement.				
	Describe what the assessor observed in the vendor evidence and discovered through interviews to conclude that the specific software functionality impacted by software updates is clearly outlined in the change summary information.				
	Summarize how the software vendor makes change details easily accessible to stakeholders.				
10.1.b For a sample of software updates, the assessor shall examine publicly available information or notifications regarding the software updates to confirm the following: • Change summary information is made available to stakeholders. • Change summary information accurately reflects the changes made to the software.	**Identify** the software updates sampled for this test requirement.				
	Identify the publicly-available information and software update notifications examined that confirm the findings for this test requirement.				

Control Objectives and Test Requirements	Reporting Instructions	Reporting Details: Assessor’s Response	Summary of Assessment Findings (check one)
	For the software updates sampled, **describe** what the assessor observed in the publicly-available information and software update notifications to conclude that change summary information was made available to stakeholders upon changes to the software.		
	For the software updates sampled, **describe** what the assessor observed in the publicly-available information and software update notifications to conclude that the change summary information provided to stakeholders accurately reflects the changes that were made to the software in the update.		

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 ROC.