Payment Card Industry (PCI)

Software Security Framework

Summary of Changes from Secure Software Requirements and Assessment Procedures Version 1.0 to 1.1

April 2021

Introduction

This document provides a summary of changes to the *PCI Software Security Framework – Secure Software Requirements and Assessment Procedures* ("Secure Software Standard") from v1.0 to v1.1. Table 1 provides an overview of the types of changes. Table 2 summarizes the material changes found in the Secure Software Standard v1.1.

Table 1: Change Types

[1]Change Type	Definition
Clarification	Clarifies intent of requirement. Ensures that concise wording in the standard portrays the desired intent of requirements.
Additional guidance	Explanation, definition and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Evolving Requirement	Changes to ensure that the standards are up to date with emerging threats and changes in the market.

Table 2: Summary of Changes

Section		Change	Type[1]
v1.0	v1.1		
General			
Various	Various	Minor updates to address errata, clarify intent, and support the addition of the Terminal Software Module.	Clarification
Various	Various	Added clarification throughout the document to differentiate software vendors from other types of vendors.	Clarification
Various	Various	Added hyperlinks to all internal references to other sections, control objectives and test requirements.	Clarification
Various	Various	Updated all references to "vendor security guidance" to "software vendor implementation guidance" to align with changes to Control Objective 12.	Clarification
Secure Software Requirements	PCI Secure Software Requirements	Added "PCI" to Secure Software Requirements section title.	Clarification
Secure Software Requirements	Requirements Overview	Moved descriptions of Secure Software Core Requirements and Module A – Account Data Protection sections to the Requirements Overview section.	Clarification
Security Objectives	Requirements Overview	Updated section title and content to remove the concept of "security objectives" as a formal document construct. Added an overview of the main requirements sections to explain how requirements are organized within the document.	Clarification
N/A	Test Platform	Added a new sub-section to explain the purpose and use of a "Test Platform".	Additional guidance
Secure Software Core Requirements			
1.2.b, 1.2.c 2.2.a, 2.2.b, 2.2.c	1.2.b, 1.2.c 2.2.a, 2.2.b, 2.2.c	Updated language in test requirements to align with language in the associated control objectives.	Clarification

Section		Change	Type[1]
v1.0	v1.1		
2.1.a 2.2.b 2.3.d 4.2.c 6.3.b 7.2.a	2.1.a 2.2.b 2.3.d 4.2.c 6.3.b 7.2.a	Updated references to software "installation" to include "initialization, or first use" to account for scenarios where software is delivered (e.g., via a service) rather than installed.	Clarification
2.1.b, 2.1.c 3.1.d 3.3.a 3.4.a, 3.4.c 3.5.a, 3.5.c 5.2.c 5.4.a 7.1.a, 7.1.b 7.4.a 8.1.a 8.3.b 9.1.a, 9.1.c, 9.1.d 10.2.a A.2.3.a	2.1.b, 2.1.c 3.1.d 3.3.a 3.4.a, 3.4.c 3.5.a, 3.5.c 5.2.c 5.4.a 7.1.a, 7.1.b 7.4.a 8.1 8.3.b 9.1.a, 9.1.c, 9.1.d 10.2.a A.2.3.a	Removed unnecessary or improper internal references.	Clarification
2.1.e 7.1.b	2.1.e 7.1.b	Changed reference in notes from "threat model" to "threat information."	Clarification
2.3.a, 2.3.d, 2.3.e 3.1.a, 3.1.b 3.2.a, 3.2.b 5.1.a, 5.3.a 6.1.b 6.2.b 7.1.e	2.3.a, 2.3.d, 2.3.e 3.1.a, 3.1.b 3.2.a, 3.2.b 5.1.a, 5.3.a 6.1.b 6.2.b 7.1.e	Clarified language in the notes in test requirements with internal references to other control objectives.	Clarification
3.4	3.4	Removed improper reference to ISO 27038 in guidance.	Clarification
3.6.b	3.6.b	Updated incorrect test requirement reference from 3.2.a to 3.6.a.	Clarification

Section		Change	Type[1]
v1.0	v1.1		
4.1	4.1	Updated the note in Control Objective 4.1 to clarify that it should be validated at the same time as Control Objective 10.1 since it is an extension of 10.1. This change was implemented to align with similar references in the Terminal Software Module.	Clarification
5.2	5.2	Updated the note in guidance to clarify the referenced control objectives cover "sensitive functions" and "sensitive resources" in addition to "sensitive data."	Clarification
6.2.c 6.3.b 7.4.c 9.1.d	6.2.c 6.3.b 7.4.c 9.1.d	Simplified the language in the test requirement.	Clarification
7.1.c 7.4.a	7.1.c 7.4.a	Replaced references to "DSS" with "digital signature".	Clarification
7.3 8.2	7.3 8.2	Clarified language in guidance.	Clarification
12	12	Changed the name of Control Objective 12 from "Vendor Security Guidance" to "Software Vendor Implementation Guidance" to clarify intent.	Clarification
Module A – Account Data Protection	Module A – Account Data Protection Requirements	Renamed section title from "Account Data Protection" to "Account Data Protection Requirements". Added new summary table and a new "Purpose and Scope" section at the beginning of the module to describe the module's purpose and applicability.	Additional guidance
N/A	Module B – Terminal Software Requirements	New requirements module for software intended for deployment and execution on payment terminals (i.e., PCI-approved POI devices).	Evolving requirement