Payment Card Industry (PCI)
Data Security Standard

Summary of Changes from Template for Report on Compliance for use with PCI DSS v3.0 - Version 1.0 to 1.1

July 2014

Introduction

This document provides a summary of changes for the Template for Report on Compliance for use with PCI DSS v3.0 Version 1.0 to 1.1. Table 1 provides an overview of the types of changes included in the Template for Report on Compliance for use with PCI DSS v3.0 Version 1.1. Table 2 provides a summary of material changes to be found in the Template for Report on Compliance for use with PCI DSS v3.0 Version 1.1.

Table 1: Change Types

Change Type	Definition
Clarification	Clarifies intent of instructions. Ensures that concise wording in the reporting template portrays the desired intent of instructions.
Additional Guidance	Explanation, definition and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Correction	Changes to remedy typos or similar edits

Table 2: Summary of Changes

Section		Change	Type
Template v1.0	**Template v1.1**		
Cover page/ Document Changes	Cover page/ Document Changes	Removal of random "c" from cover page. Edited to reflect increase in versioning (to 1.1) and tracked in Document Changes. Updated month in footer.	Correction
Introduction to the ROC Template	Introduction to the ROC Template	Changed "Executive Summary" to "Summary Overview" to remedy confusion with the intention of detail required here. Impacts references at p.9 (2.1) and p.22 (5.1) as well. Removed "X" in box for In Place in the "Requirement X: Sample" content. Added "against PCI DSS v2.0 (or PCI DSS v3.0)" in the sample response for addressing dependence on another service provider's compliance.	Clarification
Introduction to the ROC Template	Introduction to the ROC Template	Added instruction: "Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as the report is written and for the recipient in understanding the context the responses and conclusions are made. Addition of text or sections is applicable within reason, as noted above. Refer to the "ROC Reporting Template for PCI DSS v3.0: Frequently Asked Questions (FAQs)" document on the PCI SSC website for further guidance." Added table (with context instructions and FAQ reference) from FAQ to explain the difference between in place, in place with CCW, not applicable, not tested and not in place. Combined with already present guidance, including adding a column to the table to include the guidance for the sample that was already present. Text was created for In Place with CCW, N/A, and Not Tested to go with the sample. Changed "Do's and Don'ts: General Guidance and Best Practices" to "Do's and Don'ts: Reporting Expectations" to strengthen this as expectation (and not suggestion).	Additional Guidance
Introduction to the ROC Template	Introduction to the ROC Template	Correction from "payment application" to "assessed entity." Added Q21 from FAQ on ROC Reporting to remediate stance on Future-Dated Requirements (which has changed from "Not Tested" to "Not Applicable" from 1.0 to 1.1). Edited content to reflect the shift in expectation for future-dated requirements (not applicable instead of not in place). Deleted confusing text about similar text. Removed erroneous statement from "Not Tested" original guidance -"This could also be used where an entity is being assessed against 3.0, but the third-party service provider they are using is only compliant to 2.0. See guidance for this under "ROC Reporting Details." Corrected the reference at "Sections 2.8, "Documentation Reviewed," and 2.9 "Individuals Interviewed" to Sections 4.10 and 4.11.	Correction
Section 1: Contact Information and Report Date	Section 1: Contact Information and Report Date	Added Section 1.4: Additional Services Provided by QSA Company, with two responses required. Consistent with the Validation Requirements for QSAs v1.2, Section 2.2 "Independence." Added sample of PCI credentials to show what it being asked for there (QSA, PA-QSA, etc.)	Clarification

Section 1: Contact Information and Report Date	Section 1: Contact Information and Report Date	Added "for this specific report (not the general QA contact for the QSA)" to "Assessor Quality Assurance (QA) Primary Reviewer" to discourage companies from plugging in the name of the head of QA who never saw the report, align expectations/better accountability	Additional Guidance
Section 1: Contact Information and Report Date	Section 1: Contact Information and Report Date	Added missing response box at "Assessor PCI Credentials" on p.8	Correction
Section 3: Description of Scope of Work and Approach Taken	Section 3: Description of Scope of Work and Approach Taken	Removal of footnote in 3.4 that didn't lead to anything	Correction
Section 3: Description of Scope of Work and Approach Taken	Section 3: Description of Scope of Work and Approach Taken	Added text at 3.1 Assessor's validation of scope accuracy to clarify what type of response is needed and to acknowledge where the assessor, assessed entity or both may be completing the action. Added text to the scope attestation "to the best of the assessor's ability and with all due diligence" Added note at 3.2 Environment on which the assessment is focused to clarify the intent of "people" and "technologies" here for reporting. Added instructions for the assessor to include additional reporting for the brands/acquirers (as required by them) at 3.5 or as an appendix.	Clarification
Section 4: Details about Reviewed Environment	Section 4: Details about Reviewed Environment	Added "and for what purpose it is used" to the column header "Describe how cardholder data is transmitted and/or processed" to clarify the detail expected here. Added "database" to the examples under the "Data Store" column header since it is noted in the instructions with the tables and files. Added "latest version date" under "Document Date" to clarify intended detail at 4.10: Documentation Reviewed. Changed "tested procedure" to "testing procedure" to clarify original intent in the table headings at 4.13 and 4.14. Added instructions for homegrown components and software/applications at 4.4 Critical Hardware at 4.5 Critical Software. Added instructions for homegrown payment applications/solutions at 4.9 Third-party payment applications/solutions.	Clarification
Section 4: Details about Reviewed Environment	Section 4: Details about Reviewed Environment	Removed the third bullet under "If sampling is used" in 4.6 Sampling, as the question was determined to be redundant.	Correction

Section 6: Findings and Observations

Requirement	Change	Type
1.1.7.b	Removed an extraneous row regarding interview where content was present again in the next row.	Correction
2.1.1.a	Reformatted table so the text of 2.1.1.a doesn't cut off; this change inadvertently remedied the same issue at 2.1.1.c	Correction
3.2	Changed grey box there, as it could possibly be n/a if there is no SAD at all.	Correction
3.2.3, 6.5.9	Remedied error where the boxes for N/A and Not Tested were merged into one.	Correction

3.5.2.a, 3.5.2.b	Addressed confusion from the testing procedure identifying HSM as "host security module" by replacing "host" with "host/hardware" – glossary refers to both host and hardware.	Clarification
4.2.b	Corrected the "if yes" and "if no" order – "if yes" should have been first and been with the instruction for unprotected PAN, "if no" should have been second and been with the instruction for all PAN.	Correction
6.4.4.b	Removed "test" from "sample of test data" to accurately reflect what is being examined at this testing procedure.	Correction
8.7.b	Corrected error where it said "use" instead of "user" in the second bullet of both lists.	Correction
10.2	Error at 4th bullet remedied in both lists (should be "Invalid logical access attempts")	Correction
10.2	Edited 5th bullet to better reflect 10.2.5, including the supporting sub-bullets, in both lists	Clarification
11.2.2.b	Corrected error where it said "internal" where it should have said "external" in the instructions.	Correction
11.3.1.b, 11.3.2.b	Corrected errors where it said "scans" and should have been "penetration tests" or "test."	Correction