Payment Card Industry

Data Security Standard

PCI DSS v4.x: Items Noted for Improvement (INFI) – Instructions and Worksheet

June 2023

Completing the *PCI DSS v4.x Items Noted for Improvement (INFI) Worksheet*

Introduction

It is common during a PCI DSS assessment for the assessor to identify PCI DSS requirements that are not fully in place or security controls that have not been consistently maintained in accordance with a requirement. When this occurs, and if the entity has implemented corrective action to successfully address the identified issues prior to completion of the assessment, the assessor can reassess the controls to determine whether the requirement is now fully in place.

Performing corrective actions to address identified issues and reassessing requirements to verify that the issues have been fully addressed are common aspects of the PCI DSS assessment process.

Items identified as needing corrective action may be considered In Place only after the assessor has verified that the reason for the failure has been addressed, and that controls and processes intended to both prevent reoccurrence of the failure and fully meet the requirement have been implemented.

Assessors are required to:

- Document all items that needed corrective action in the Items Noted for Improvement (INFI) Worksheet,
- Complete and sign the Assessor Acknowledgment and Attestation section of the Worksheet, and
- Provide the completed and assessor-signed Worksheet to the entity.

The INFI Worksheet is required to be completed by Qualified Security Assessors (QSAs) as part of all PCI DSS v4.0 assessments. Completion of the INFI Worksheet is recommended, but not required, for PCI DSS v3.2.1 assessments.

Requirements that the assessor validated as being in place after the entity had implemented the necessary corrective action are reported as In Place in the applicable validation document—for example, the ROC.

Refer to the following additional documents on the PCI SSC website for more information about use of the INFI Worksheet:

- *PCI DSS v4.x: Items Noted for Improvement (INFI) Worksheet – Frequently Asked Questions.*
- *PCI DSS v4.x: Items Noted for Improvement and Compensating Controls Guidance*

Use of this Worksheet

This Worksheet provides a consistent method for assessors to document corrective action and reassessment activities during the assessment process.

This Worksheet is intended for internal use between the assessor and the assessed entity. It is intended to help entities better understand their security posture, improve their security processes and controls, and identify areas for improvement as they work towards security as a continuous process. The

Worksheet also provides a useful method for entities to report items needing improvement and associated corrective actions to senior management.

It is good practice for entities to maintain this document and share it internally with the compliance and risk departments within their organization. Entities are encouraged to share the Worksheet externally with assessors and other third parties, as it is an effective tool to allow future assessors and third parties to understand past challenges and how they were addressed.

QSAs are required, and ISAs are strongly encouraged, to maintain copies of this Worksheet as part of their assessment workpapers.

Example Usage

Use of the Items Noted for Improvement Worksheet applies to all types of PCI DSS requirements. This includes scenarios where:

- The assessor is validating that a control has been performed periodically or at a defined frequency.
- The assessor is validating that a control is in place at a single point in time.

The requirement for assessors to identify and document items noted for improvement does not change how the assessor performs testing procedures or selects samples for testing.

An example scenario for use of this Worksheet would be when an entity has missed one of their quarterly ASV scans during the past year and has since completed ASV scans that meet the applicable PCI DSS requirements, determined why the scan was missed in the past, and has implemented controls and processes to prevent scans from being missed in the future.

Other examples* might include:

- A critical security patch was not applied within 30 days, or was not applied to all affected systems, and was detected by the entity during their next quarterly scan and immediately installed.
- A misconfigured network security control was identified by the assessor during the assessment, which the entity corrected, and the assessor verified prior to completion of the assessment.
- A missing or inadequate policy document was noticed at the start of the assessment, which the entity immediately updated, and the assessor verified prior to completion of the assessment.
- Prior to the assessment, a non-critical device was accidentally excluded from PCI DSS scope and was not configured per the entity's PCI DSS configuration standards prior to going into production, but the device was checked and updated with the correct configuration a month after going into production.
- A small number of staff had not completed the entity's security awareness training in more than 12 months, but all had finished the training by completion of the assessment.

* *These examples are not all inclusive. They do not exclude other requirements from being noted as needing improvement, nor do they suggest these requirements are expected to need improvement.*

This Worksheet applies to all requirements that needed corrective action before they could be verified as being In Place, regardless of whether it was the entity or the assessor that initially identified the requirement(s) as not being in place.

Note: *It is the assessor's decision as to whether it is appropriate to leverage the INFI worksheet or, in cases where the entity has significant and/or multiple failures in their controls, to issue a Not in Place finding.*

Reporting

To determine that a requirement initially found to be not in place has been properly addressed by the entity and can now be considered fully in place, the assessor must verify that the entity has:

1. Identified and addressed the reason why the requirement was not met.
2. Implemented and documented the controls and processes needed to fully meet the requirement.
3. Implemented and documented ongoing processes intended to prevent reoccurrence of the control failure.

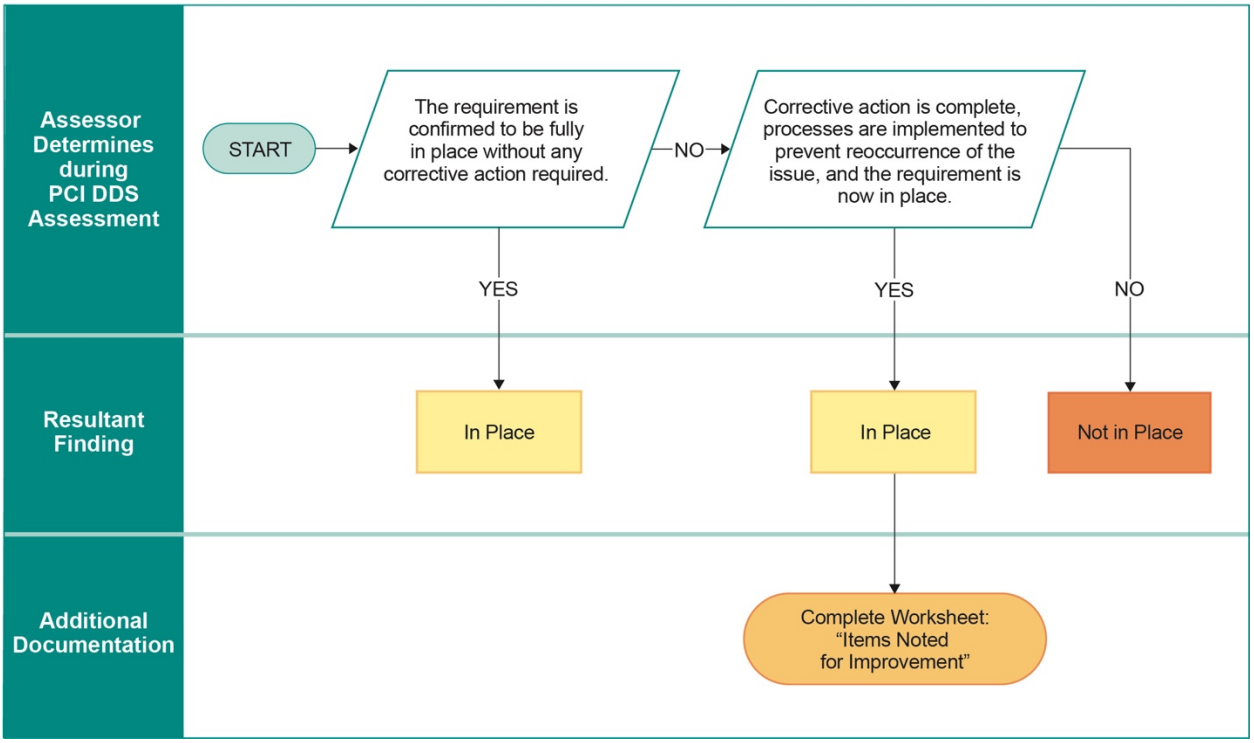
This Worksheet and all supporting evidence reviewed and collected by the assessor is expected to form part of the assessor's Workpapers (as defined in the *QSA Qualification Requirements* and the *QSA Program Guide*).

PCI DSS requirements are ***not*** considered to be "In Place" if corrective actions are not yet fully implemented or are scheduled to be completed at a future date. PCI DSS requirements are also not considered "In Place" if the assessor has not validated items 1-3 above.

Any requirements that have not been fully satisfied must be reported as "Not in Place."

Figure N illustrates how the assessor determines whether a requirement is "In Place" and the resultant reporting.

Figure N: *Determining an "In Place" Finding*



Assessor Requirements

QSAs are required to:

- Complete the Worksheet and sign the Worksheet Attestation.
- Deliver a completed and signed copy of the Worksheet and Attestation to the assessed entity. These documents must be provided to the entity, preferably to an individual with an appropriate level of authority, for example, the Executive Officer who signed the AOC, the individual responsible for oversight of the entity's compliance program, or a member of the entity's senior executive team.[1]
- Retain a completed and signed copy of the Worksheet, Attestation, and supporting evidence with their assessment workpapers.

QSAs must complete and sign the *Assessor Acknowledgement and Attestation* section of the Worksheet Attestation and provide a copy of the Worksheet and signed Attestation to the assessed entity before they sign off on the ROC/AOC.

The *Assessor Acknowledgement and Attestation* section must be completed even if there are no items noted for improvement in the Worksheet.

ISAs are strongly encouraged, but not required, to follow these practices.

Completion of the INFI Worksheet is recommended, but not required, for PCI DSS v3.2.1 assessments.

Completion of the INFI Worksheet is recommended, but not required, for assessments that are reported via a Self-Assessment Questionnaire (SAQ). Where a QSA is performing testing for a SAQ, they are expected to apply the same level of due diligence to the assessment process, including the identification of any issues needing corrective action.

These INFI requirements for QSAs are documented in the QSA Program Guide and QSA Qualification Requirements.

[1] Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the organizational structure.

How to Complete the Items Noted for Improvement Worksheet

The following table describes the column headings and includes examples of the responses expected for each item noted in the INFI Worksheet on the next page.

***Table 1:** INFI Worksheet Components*

INFI Worksheet Column Heading	Description of Information Required
Requirement #	PCI DSS Requirement number.
Issue Identified by	Indicate whether the entity or the assessor identified the need for corrective action.
Description of Issue	Which aspect(s) of the requirement was noted as needing corrective action? *For example, describe which controls or processes were not properly implemented or were not applied to all in-scope system components. Identify the affected components and the period of time that the controls were not implemented.*
Cause of Failure	What caused the failure that resulted in the need for corrective action? *For example, describe what caused the control or process to not be properly implemented or to not be applied to all in-scope system components.*
Corrective Action Taken	Describe the corrective action(s) taken by the entity that resulted in the requirement being In Place. *For example, which actions were performed by the entity that resulted in the control or process being properly documented and implemented and applied to all in-scope system components*.
Preventive Action Taken	Describe the actions taken by the entity to help prevent reoccurrence of the failure. *For example, which controls/processes the entity documented and implemented to address the cause(s) of the failures and provide assurance that the requirement will continue to be properly implemented and applied to all in-scope system components.*

PCI DSS v4.x – Items Noted for Improvement Worksheet

This Worksheet is to be completed by the assessor for all requirements that were initially found to be not in place but were addressed by the entity and verified by the assessor to be fully in place prior to completion of the assessment. Refer to Table 1 above for direction on how to complete this Worksheet.

Requirement #	Issue Identified by:		Description of Issue	Cause of Failure	Corrective Action Taken	Preventive Action Taken
	Entity	Assessor				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				

PCI DSS v4.x INFI Worksheet Acknowledgement and Attestation

In accordance with the QSA Program Guide and Qualification Requirements, QSAs are required to complete and sign the INFI Worksheet Acknowledgement and Attestation and provide a copy of both the Worksheet and this signed Acknowledgment and Attestation to the assessed entity before they sign off on the ROC/AOC*. ISAs are encouraged, but not required, to follow these INFI Worksheet practices as well.

Assessor Acknowledgment and Attestation

Assessor signatory(s) confirms:

Were items noted for improvement during the Assessment?		☐ Yes	☐ No
If Yes: Confirm for all items identified in this Worksheet:			
☐	The entity has corrected all items and the requirement(s) is verified as being fully in place.		
☐	Controls and processes to meet the requirement(s) are properly implemented and applied to all in-scope system components.		
☐	Controls and processes are implemented to prevent reoccurrence of the identified failure(s).		
☐	This completed and signed Worksheet has been provided to:		
	Entity Representative Name:		
	Entity Representative Job Title:		
	On:	YYYY-MM-DD	

Signature of Lead Assessor ↑	Date: YYYY-MM-DD	
Lead Assessor Name:		
Lead Assessor Qualification (select one)	☐ ISA	☐ QSA

Entity Acknowledgment of Receipt*

Entity acknowledges:
For all items identified in this Worksheet:

☐	This Worksheet was received from the assessor as noted above.
☐	The cause(s) of failures that resulted in items noted for improvement has been addressed.
☐	The corrective actions identified in the Worksheet to address the items noted for improvement and to help prevent reoccurrence of the identified failures have been implemented.

Signature of Entity Representative ↑	Date: YYYY-MM-DD
Entity Representative Name:	Entity Representative Title:

** The entity is not required to complete the Entity Acknowledgment of Receipt in order for the assessor to sign off on the ROC/AOC.*