Payment Card Industry (PCI)

Data Security Standard

PCI DSS v4.x: Items Noted for Improvement (INFI) Worksheet – Frequently Asked Questions

June 2023

Purpose of Document

The *PCI DSS v4.x: Items Noted for Improvement Worksheet* (INFI Worksheet) is intended for internal use between the assessor and the assessed entity 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. This document addresses questions around the use of the *PCI DSS v4.x INFI Worksheet.*

1. General Questions

Q 1.1 What is the purpose of the *PCI DSS v4.x Items Noted for Improvement (INFI) Worksheet*?

A *To provide a consistent method for assessors to document corrective action and reassessment activities during an assessment period, and to provide a consistent tool to facilitate related conversations between the assessor and the assessed entity.*

Q 1.2 Does this Worksheet need to be completed for PCI DSS v3.2.1 assessments?

A *No, this Worksheet is intended for PCI DSS v4.x assessments. Completion of the INFI Worksheet is recommended, but not required, for PCI DSS v3.2.1 assessments.*

2. Assessor Responsibilities

Q 2.1 Are QSAs required to complete an INFI Worksheet for every PCI DSS v4.x assessment?

A Yes.

Q 2.2 Are QSAs required to complete an INFI Worksheet even if there are no Items Noted for Improvement?

A *Yes, QSAs are required to complete the Assessor Acknowledgement and Attestation section even if there are no items noted that needed improvement during the assessment, in which case the QSA will check the "No" box in that section.*

Q 2.3 Are ISAs completing a Report on Compliance for their organization required to complete an INFI Worksheet?

A *ISAs are encouraged, but not required, to complete an INFI Worksheet.*

Q 2.4 Can the QSA still sign the Attestation of Compliance (AOC) if an entity refuses to receive the INFI Worksheet?

A *Yes, the QSA is still required to sign the AOC. The INFI worksheet is not considered a compliance document, so whether the entity receives it does not affect the QSA's obligations to complete and sign the AOC. In this scenario, the QSA should also document in the workpapers that the entity refused to accept the INFI Worksheet.*

Q 2.5 Are QSAs required to complete INFI Worksheets when they assist entities with SAQs?

A *No. If a QSA assists an entity in completing their SAQ, (for example, by testing requirements to determine if they are met), the QSA's due diligence should include identification of any issues that need corrective action. It is recommended, but not required, that a QSA completes an INFI Worksheet to document any such issues noted as part of SAQ completion.*

3. Use of the INFI Worksheet

Q 3.1 How should assessed entities use the INFI Worksheet?

A *It is good practice for entities to maintain this document and share it internally with the compliance and risk departments within their organization. Entities may also choose 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.*

Q 3.2 Why does the INFI Worksheet include whether a control failure was first identified by the entity or the assessor?

A *Entities with established processes to identify control failures and implement corrective actions within their environments generally have more mature risk management and security processes, with information about whether those processes are operating effectively. While entities are not required to self-identify failures for use of an INFI worksheet, the INFI worksheet does include a section to identify whether the failure was first identified by the entity or the assessor. Including whether the control failure was identified by the entity or the assessor is intended to help entities understand whether they are effectively maintaining and monitoring their controls and environment.*

Q 3.3 What is the role of INFI for requirements with a periodic or defined frequency, where an entity did not perform the activity within the required timeframe?

A *Several PCI DSS requirements specify that a security activity is to be performed periodically or at a defined frequency. If an entity fails to perform the control on one or more of the defined timeframes, there is no way for them to perform the control retroactively or backdate a later occurrence of the control to an earlier period.*

A common example is external ASV scans, which are required at least once every three months. If an ASV scan was not performed for six months, the entity will not have sufficient ASV scan reports to provide as evidence during the assessment. Other examples include not installing a critical security patch within 30 days of release and not reviewing network security control configurations at least once every six months.

In these scenarios, the assessor can use the INFI Worksheet to support a finding of "In Place" if the entity has implemented corrective actions and successfully performed the control in accordance with the requirement, and the assessor has assurance that:

- *The entity has a repeatable and documented process for performing the control,*
- *The entity demonstrates that the activity was missed due to an exceptional circumstance (poor security practices and recurring failures are not an "exceptional circumstance"),*
- *The entity shows that they have addressed the issue that led to the exception, and*
- *The entity has included steps in their process to prevent recurrence.*

If the entity cannot demonstrate the above, or the assessor does not have assurance that the entity has processes in place to meet the requirement, the assessor can consider whether a "Not in Place" finding would be the appropriate result.

Q 3.4 What should a QSA do if they observe the same item is noted for improvement during the next assessment?

A *The intent of the INFI Worksheet is 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 entity is expected to address items noted for improvement, including implementing processes to prevent recurrence. However, it is not intended to be an automatic "Not in Place" finding if that same item is noted for improvement during the next PCI DSS assessment.*

The assessor has discretion when deciding how to report repeated items noted for improvement, considering the following:

- *Were the processes previously implemented by the entity to prevent recurrence of the item ineffective or not followed?*
- *Were the circumstances or reasons for the current failure different than for the previous failure (for example, the failure happened in a different part of the company or a different set of systems that fall under separate processes, or the failure happened for a completely different reason)?*

If the assessor sees a recurring theme and determines that the current failure resulted from a failure of the processes previously developed by the entity to prevent recurrence, a "Not in Place" result may be the appropriate finding.

Q 3.5 Does use of the INFI Worksheet apply to all PCI DSS requirements?

A *Yes. Use of the INFI Worksheet applies to all PCI DSS requirements, including 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.*