Payment Card Industry

Data Security Standard

PCI DSS v4.x: Items Noted for Improvement and Compensating Controls Guidance

June 2023

Purpose of Document

PCI DSS includes a few approaches for assessed entities to provide evidence to their assessors about how PCI DSS requirements are met. Two of those approaches, Compensating Controls and Items Noted for Improvement, are addressed in this document.

Overview: Compensating Controls

Compensating Controls have been present in PCI DSS since the inception of the standard. It is intended to help assessed entities address the risk when there is a technical or business constraint that prevents meeting the PCI DSS requirement as stated. Use of Compensating Controls is documented in the validation documents: the *Report on Compliance (ROC)* or the *Self-Assessment Questionnaire (SAQ),* and the *Attestation of Compliance (AOC)* that is affiliated with the ROC or SAQ.

For more information about the use of Compensating Controls, refer to Appendices B and C in PCI DSS on the PCI SSC website.

Overview: Items Noted for Improvement

Items Noted for Improvement (INFI), a new concept for PCI DSS v4.0, is meant for internal use between the assessor and the assessed entity when a PCI DSS requirement was not initially met, but where the entity has taken steps to address the failure and ensure that the requirement is met going forward. 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. Items Noted for Improvement are documented in an INFI Worksheet. This Worksheet also provides a useful method for entities to report items needing improvement and associated corrective actions to senior management.

For more information about the use of the INFI Worksheet, refer to the following documents on the PCI SSC website:

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

This document addresses use of Compensating Controls and Items Noted for Improvement as part of PCI DSS v4.x assessments.

PCI DSS v4.x: Items Noted for Improvement and Compensating Controls Guidance

Topic	Compensating Control (CC)	Items Noted for Improvement (INFI)
Purpose	Entity identifies a **technical or business constraint** that prevents it from meeting the requirement as stated.	Entity or assessor identifies **one or more items that require corrective action** before the assessment is complete for that requirement to be considered In Place.
General characteristics	▪ Proactive development of mitigating actions. ▪ The PCI DSS requirement is not met as stated, but an alternate control is implemented to address the risk. ▪ Can be a long-term approach, with annual confirmation that the technical or business constraint still exists. ▪ Can be a short-term approach to address a short-term risk.	▪ Reactive correction to a missing control or event. ▪ The PCI DSS requirement is met after the correction is applied. ▪ Short term approach, with long term remediation that prevents recurrence of the failure.
Entity's role	▪ Identify the technical or business constraint that prevents meeting the requirement. ▪ Design an alternate (compensating) control that meets the criteria in PCI DSS Appendix B. ▪ Implement the control. ▪ Document the control in a Compensating Control Worksheet (CCW) per PCI DSS Appendices B and C.	▪ Identify and address the reason the requirement was not met (what failed). ▪ Implement controls and processes to meet the requirement going forward. ▪ Implement controls and processes to prevent (or detect) reoccurrence of the failure.

Topic	Compensating Control (CC)	Items Noted for Improvement (INFI)

Assessor's role	▪ Have conversations and review the CCW completed by the entity to understand the technical or business constraint, etc.
	▪ Assessor may assist with development and documentation processes.
	  • Must consider independence factors if assessor helps develop the CC.
	▪ Evaluate the CC and perform testing to determine if it is sufficient to consider the requirement In Place.
	▪ If CC is sufficient:
	  • Document the CCW in the ROC or SAQ.
	  • Record an In Place result in the ROC or SAQ.
	  • Keep CCW and supporting evidence in workpapers.
	▪ If CC is not sufficient:
	  • Record a Not in Place result in ROC or SAQ.
		▪ Have conversations with entity about the noted item, corrective actions needed, etc.
		▪ Verify the entity has:
		  • Addressed the reason for the failure,
		  • Implemented controls to meeting the requirement going forward,
		  • Implemented controls and processes to prevent (or detect) reoccurrence.
		▪ If efforts to address item are sufficient:
		  • Document all in the INFI Worksheet.
		  • Record an In Place result in the ROC or SAQ.
		  • Provide INFI Worksheet to entity.
		  • Retain INFI Worksheet and supporting evidence in workpapers.
		▪ If item is not addressed sufficiently:
		  • Record a Not in Place result in ROC or SAQ.

Example use case: Missing ASV scan	Due to unexpected circumstances, the entity needed to change their ASV vendor right before scans were planned for the quarter. In preparation for this change, the entity **proactively** implemented a compensating control to address any risk until their new scan vendor could start performing scans: ▪ Internal staff to scan the external systems daily and quickly address any high risk or critical vulnerabilities. ▪ Finding a new ASV vendor was prioritized and external ASV scans were again available within two weeks.	Due to lack of proper planning, the entity failed to perform one or more ASV scan(s) during the past year. Once identified, the entity's **reaction** to the failure was to put controls and processes in place to complete ASV scans going forward and to mitigate the chance of missing ASV scans in the future: ▪ The entity determined what caused the missed scans (the assigned staff person forgot to initiate the scans). ▪ The entity began sending automatic notifications to several staff members immediately if an ASV scan was not performed on time. ▪ The entity implemented monthly ASV scans going forward to increase the chance of having four passing ASV scans during the year. ▪ The entity implemented monthly reporting to upper management about ASV scan status and timely vulnerability resolution.