

Can a compensating control be used for requirements with a periodic or defined frequency, where an entity did not perform the activity within the required timeframe?

PCI SSC FAQ | Article 1572 | June 2025

No.

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 missed, 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, an assessor can determine a requirement to be “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 “exceptional circumstances”),
- 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 continue to meet the requirement, the assessor can consider whether a “Not in Place” finding would be the appropriate result.

To document these situations, assessors should follow assessment best practices to determine whether a requirement can be considered in place, and document it in their work papers and in the Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ). This should include the corrective actions the entity implemented, that the entity has successfully performed the control in accordance with the requirement, and how the assessor has assurance that the entity meets the bullets outlined above.