WHITE PAPER

PCI DSS 4.0 Changes: Compliance Timeline Clarifications

JUSTIN BONK, CISSP, PCI-QSA, CIPP / US, CIA, CFE, CISA
SENIOR MANAGER, RISK ADVISORY SERVICES

PCI DSS 4.0 adds specificity regarding timeframes used in assessment.

In PCI DSS 3.2.1, timeframes such as weekly, monthly or quarterly were left undefined, leaving it to interpretation as to the specific frequency that an activity was required. Timeframes for sub-requirements are now explicitly defined, narrowing the window of time you'll have to perform required processes.

FREQUENCY	SPECIFIC TIMELINE
Daily	Every day of the year (not only on business days.)
Weekly	At least once every seven days.
Monthly	At least once every 30 to 31 days, or on the nth day of the month.
Every 3 months ("Quarterly")	At least once every 90 to 92 days, or on the nth day of each third month.
Every 6 months	At least once every 180 to 184 days, or on the nth day of each sixth month.
Every 12 months ("Annually")	At least once every 365 (or 366 for leap years) days or on the same date every year.

There are many activities impacted by this clarification, including log reviews, internal vulnerability scans, ASV scans, wireless scanning, data deletion, rule set reviews, segmentation testing, security training and response plan testing. If you miss a window to perform an activity, your assessor may not have any options outside of marking the sub-requirement as 'Not in Place.'

Additionally, imprecise terms such as periodically, immediately and promptly, have been given more precise definitions, although they are still relatively subjective.

FREQUENCY	SPECIFIC TIMELINE
Periodically	Frequency of occurrence is at the entity's discretion and is documented and supported by the entity's risk analysis. The entity must demonstrate that the frequency is appropriate for the activity to be effective and to meet the intent of the requirement.
Immediately	Without delay. In real time or near real time.
Promptly	As soon as reasonably possible.

Lastly, PCI DSS 4.0 provides a prescriptive definition of a 'Significant Change,' which was previously left up to interpretation. Per the new standard, the following activities, at a minimum, must be considered a significant change:

- New hardware, software, or networking equipment added to the CDE
- Any replacement or major upgrades of hardware and software in the CDE
- Any changes in the flow or storage of account data
- Any changes to the boundary of the CDE and / or to the scope of the PCI DSS assessment
- Any changes to the underlying supporting infrastructure of the CDE (including, but not limited to, changes to directory services, time servers, logging, and monitoring)
- Any changes to third party vendors / service providers (or services provided) that support the CDE or meet PCI DSS requirements on behalf of the entity

Significant changes may trigger reperformance of requirements, such as vulnerability scans, so it is important to be aware of these items and the impact they may have on your assessment.

Altogether, these changes mean less wiggle room in your overall PCI DSS 4.0 compliance efforts. Failure to adhere to these timelines could lead to compliance issues with your assessment.

Questions on the new PCI DSS 4.0 Compliance Timing?

Contact me for a discussion of your PCI compliance situation and approaches for meeting deadlines required by PCI 4.0. You can reach me at justin.bonk@freedmaxick.com or 716.332.2680.

Trust earned.
FreedMaxick®