BerryDunn

Are you monitoring your PCI program?

Monitoring your PCI cardholder data environment (CDE) requires constant attention. Incorporating these tasks into your ongoing operational checklist can help improve your success in meeting your PCI compliance objectives.

DAILY, IMMEDIATELY, AFTER CHANGES OR PERIODICALLY

PCI Requirement	Frequency	Task Description
3.6.4	Periodically	Change cryptographic keys that have reached the end of their crypto period
8.1.3	Immediately	Revoke access for terminated users
9.9.1	Periodically	POS POI terminal inventory
9.9.2	Periodically	Inspect device surfaces for tampering or substitution
10.6.1	Daily	Review logs and security events of all cardholder data environment (CDE) components
10.6.2	Periodically	Review logs of other system components—as set by annual risk assessment
12.10.4	Periodically	Train staff with security breach response responsibilities

WEEKLY

PCI Requirement	Frequency	Task Description
11.5	Weekly	Compare critical files using change-detection mechanisms

MONTHLY

PCI Requirement	Frequency	Task Description
6.2	Monthly	Install critical system patches

3 MONTHS, 90 DAYS AND QUARTERLY OR AFTER CHANGES

PCI Requirement	Frequency	Task Description
6.2	3 months	Install all non-critical security patches (recommended)
8.1.4	90 days	Remove/disable inactive user accounts
8.2.4	90 days	Change user passwords/passphrases
3.1 b	Quarterly	Identify and delete stored cardholder data (CHD) that has exceeded defined data retention periods.
11.1	Quarterly	Detect and identify all authorized and unauthorized wireless access points (802.11)
11.2.1	Quarterly or After Changes	Perform internal vulnerability scans
11.2.2	Quarterly or After Changes	Perform external vulnerability scans using an approved scanning vendor (ASV)

6 MONTHS, 180 DAYS, OR AFTER CHANGES

PCI Requirement	Frequency	Task Description
1.1.7	6 months	Review firewall and router rulesets

ANNUALLY OR AFTER CHANGES

PCI Requirement	Frequency	Task Description
6.5	Annually	Train developers in latest coding techniques
6.6	Annually and After Changes	Assess vulnerability of public-facing web apps
9.5.1	Annually	Review security of the backup location
9.7.1	Annually	Conduct media inventories and properly maintain accompanying logs
11.1.1	Annually	Maintain inventory of authorized wireless access points and documented business justification
11.3	Annually	Implement a penetration testing methodology
11.3.1	Annually or After Changes	Perform internal and external penetration testing

11.3.4	Annually or After Changes	Perform penetration tests on CDE segmentation controls (if used)
12.1.1	Annually or After Changes	Review security policies and update as necessary
12.2	Annually and After Changes	Perform formal risk assessment
12.6.1	Annually	Provide security training upon hire and at least annually
12.6.2	Annually	Confirm employees have read and understand security policies and procedures
12.8.4	Annually	Monitor the compliance status of service providers
12.10.2	Annually	Review and test your incident response plan

For more information on PCI compliance, its importance, and strategies to achieve it contact Matt Bria.

Check out our PCI compliance webinar at advisors.berrydunn.com/pci-compliance-webinar