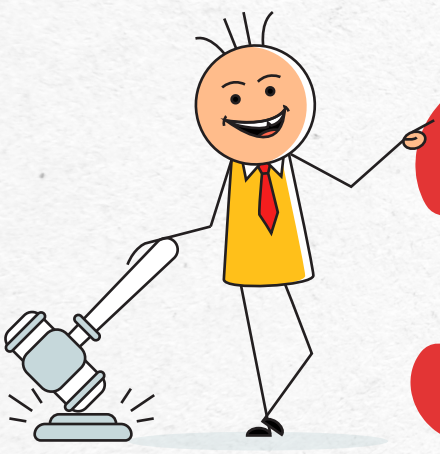
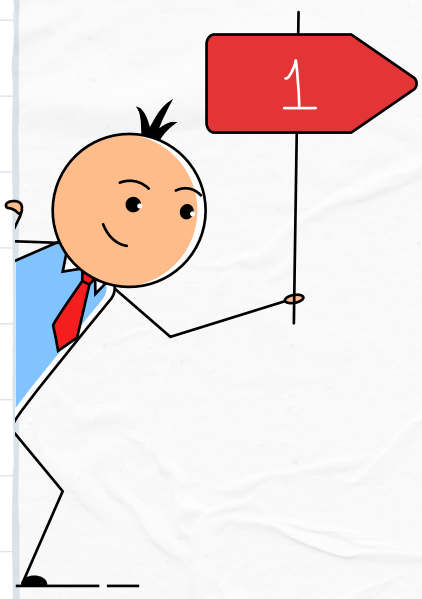
ManageEngine
Log360



3 key updates in PCI DSS 4.0

The Payment Card Industry Security Standards Council (PCI SSC) introduced the fourth edition of the PCI DSS on March 31, 2022.

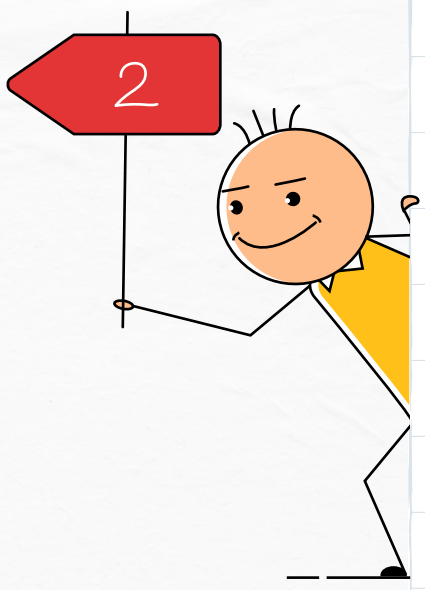
Learn about the three key updates in the regulatory standard



Option to choose a customized approach to security controls

Each objective is now accompanied by an option to follow a customized approach to security controls. Companies can choose to implement one of these options instead of the defined approach.

Stringent implementation of identity and access management measures



Requirement 8, which deals with identity and access management, has undergone considerable changes based on NIST 800-63 password guidelines.

MFA is a requirement for non-console access to the cardholder data environment (CDE) for administrators accessing all network and system components of the CDE.

For remote access, MFA can be used at either the system and application level or at the network level. While this has been specified as a best practice until 2025, it will be an audit requirement afterwards.

Comprehensive monitoring of networks using audit logs

While requirement 10 focused on implementation of audit trails and logging data pertinent to those, in the fourth version, the concept of audit trails is replaced by audit logs.

The requirement now states that organizations implement all logging mechanisms and ensure that audit logs are documented for network anomalies. The logs should also be stored for forensic analysis.

Seamlessly implement audit log mechanisms and generate audit-ready reports with Log360, a SIEM tool with compliance management features.

Get in touch

with our product experts for a free demo to learn how!

Sign up for free demo