The Latest Changes
in PCI DSS 4.0.1

Secure Script Management

Inventory, authorize, and justify all scripts on public-facing web apps, validating their integrity through regular scans to stay compliant and defend against malicious activity.

Strengthened Network Controls & Ruleset Reviews

Additional focus on Network Controls and Ruleset Reviews. Additional focus on Network configurations and controls during ruleset reviews, taking place every 6 months.

Increased Clarity for Formal Roles & Responsibilities

All roles and responsibilities are clearly defined, documented, and assigned with personnel approval.

Continuous Control Monitoring

Processes must periodically check that controls are operating effectively and monitored.

Real-Time Tamper Detection

Automated tamper detection on payment pages is required to alert personnel to unauthorized changes in security-related HTTP headers and scripts to enable rapid threat response and reduce risk.

Expanded Inventory Requirements

Software, Hardware, and third-party plugins (i.e., payment iFrames) must be more rigorously inventoried and maintained.

Comprehensive Access Reviews

Periodic scans must now be done on a regular basis based on the risk analysis of their environments and include removable media monitoring.

Updated Logging Requirements

Automated logging tools must be implemented. Additionally, all organizations are now required to detect, alert, and address failure of critical security control systems.

Our team of PCI experts will work alongside you in getting your company up to date with PCI DSS 4.0.1 compliance regulations. We can assist with every step of the audit process, from the preparation to providing coaching and guidance to your teams during the auditor interviews.

ProCern™
TECHNOLOGY SOLUTIONS

March 2022
Published

March 2024
Transition Period

March 2025
Phase in New Requirements

Contact us at:

info@procern.com