Changes coming to the PCI DSS 12 Requirements

SecurityRisk ADVISORS

PCI DSS compliance is built on 12 fundamental requirements. Below are the most significant changes coming to these essential requirements in PCI DSS v4.0 (although this is not a comprehensive list). Organizations are expected to be in full compliance of version 4.0 by March 31, 2024.

Requirement	Significant Changes
Requirement 1:	• No significant changes
Requirement 2:	• No significant changes
Requirement 3:	• All stored sensitive authentication data must be encrypted or safeguarded by merchants. • Merchants utilizing remote access technology must ensure that PAN data is not copied or relocated, not just in policies but also by employing the appropriate technology. • Disk-level encryption can no longer be used for the protection of any type of non-removable media. • Only a keyed cryptographic hash method can be used for card data protection if they choose to use a hash method.
Requirement 4:	• A new sub-requirement mandates that all merchants must maintain a record, monitor, and catalogue all SSL and TLS certificates used across public domains to enhance their validity.
Requirement 5:	• Organizations are now required to establish automatic systems and processes to identify and safeguard personnel from phishing attacks.
Requirement 6:	• A web application firewall must be installed for any web applications that are exposed to the internet. • An inventory of all known scripts used on those pages must be maintained to prevent the use of harmful scripts.
Requirement 7:	• No significant changes, but merchants are advised to enhance account reviews and review processes for systems, users, and applications.
Requirement 8:	• Strengthening of authentication measures.
Requirement 9:	• No significant changes
Requirement 10:	• Manual log reviews are no longer permitted. As this process is considered too lengthy and susceptible to mistakes, merchants must use automated review tools. • All organizations are now obligated to identify, alert, and rectify failures of crucial security control systems. This requirement was previously only for service providers but has now been expanded to all.
Requirement 11:	• A change and tamper detection mechanism for payment pages must be established.
Requirement 12:	• Merchants are required to carry out a documented scoping exercise annually or following significant changes to the scope environment. • *Immediately Effective for 4.0 Assessments*

Email: info@sra.io https://sra.io/pci-dss-v4-are-you-ready/ **Phone: (215) 867-9051**