

January 2024

Understanding and Preparing for PCI DSS 4.0

Tari Schreider



Prepared for:

imperva



Table of Contents

Introduction 2

DSS PCI 4.0 Overview..... 6

 What’s New in PCI DSS 4.0? 7

 New Requirements in Effect Now..... 8

 Future-Dated New Requirements..... 8

Cybersecurity Technologies to Achieve Compliance 14

Conclusion 17

List of Figures

Figure 1: PCI DSS Security Compliance Model..... 4

Figure 2: PCI DSS 4.0 New Requirements by Category 7

Figure 3: PCI DSS 4.0 New Requirements by Subcategory 8

List of Tables

Table A: Future Date Technical Requirements..... 9

Table B: PCI DSS Good Practices 14

Introduction

One of the most important and impactful releases of the Payment Card Industry Data Security Standard (PCI DSS) was published on March 31, 2022, through its 4.0 release. This release addresses some of the most critical architectural, control, and design risks organizations face when accepting and processing payment card transactions.

The new version of PCI DSS requires compliance with 64 new requirements by March 31, 2025. Thirteen require compliance immediately for organizations opting for version 4.0 assessments. However, some good news is that they're related to improved documentation. The broad scope of this release has caused 90% of PCI DSS decision-makers to be concerned with meeting the deadline.¹

This version marks the first time PCI allows an organization to decide on how best to comply with the standard. However, the burden of proof will be on the organization to demonstrate the effectiveness of its approach. PCI has also moved from snapshot control compliance to continuously monitoring security posture to prove risk management effectiveness and outcomes. Cybersecurity and fraud management are emerging as a fused discipline as an acknowledgment that the two are inexorably linked. This release will challenge organizations to transform their current approach to protecting cardholder data and focus on risk outcomes, not passing assessments.

PCI DSS is primarily enforced by the global card networks (American Express, Discover, Mastercard, Visa), where fines for noncompliance can range from US\$5,000 up to US\$100,000 monthly, depending on volume and the length of noncompliance. Data breach fines can include fines of US\$50 to US\$90 per customer. States, including Nevada, have amended their law on the Security of Personal Information to require Nevada businesses to comply with the PCI DSS in any transaction where the business accepts a credit or payment card.² Failure to comply could also be a basis for class action lawsuits and being expelled by one or more card networks.

¹ "The State of Enterprise Readiness for PCI DSS 4.0," S&P Global Market Intelligence, August 2023, accessed October 10, 2023, <https://www.bluefin.com/resources/white-papers/pci-dss-4-0/#/download>.

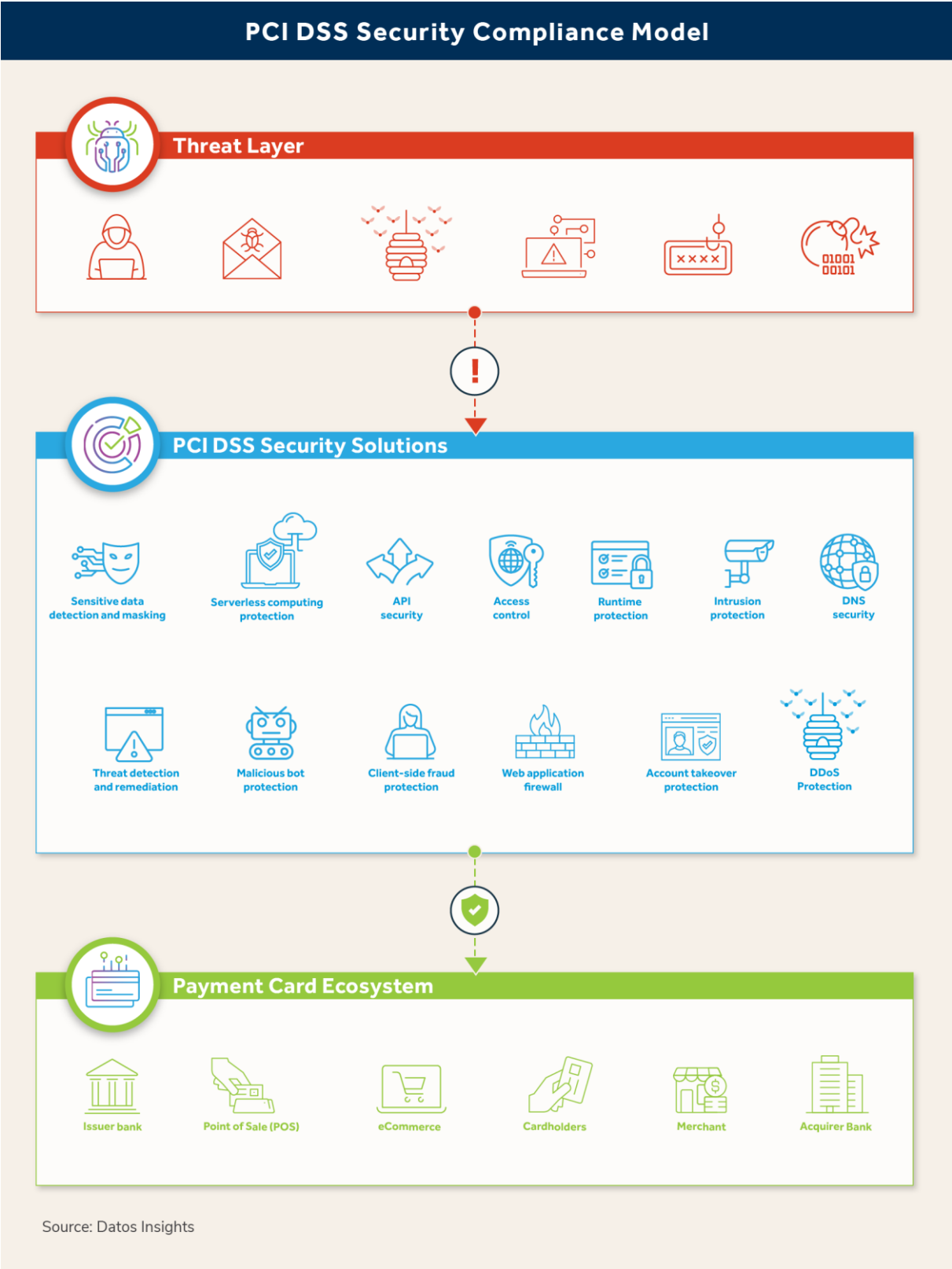
² Mauricio F. Paez, "Nevada Imposes New Requirements for Credit Card Transactions and Data Transfers," Jones Day, July 2009, accessed December 12, 2023, <https://www.jonesday.com/en/insights/2009/08/nevada-imposes-new-requirements-for-credit-card-transactions-and-data-transfers>

PCI DSS version 4.0 allows organizations to phase compliance over two years in three stages. Owing to the complexity of changes, the PCI Council allows one more year than previously for versions 2.0 to 3.0. The first stage is effective now and includes 13 new requirements that must be included for all organizations accessing against version 4.0 of the required PCI DSS Report on Compliance or Self-Assessment Questionnaire.

Stage 2 takes effect on March 31, 2024, upon the retirement of the current 3.2.1 version. Beginning April 1, 2024, all assessments must be under PCI DSS 4.0. The third and final stage requires the 51 best practices in place by April 1, 2025.

Figure 1 is an abstract view of how a single integrated solution, such as a web application and API protection (WAAP) solution, can address many risks to the payment card ecosystem.

Figure 1: PCI DSS Security Compliance Model



Organizations involved in the payment card transaction process are required to comply with version 4.0, including financial institutions, merchants, and service providers.

PCI DSS is coming, and this guide introduces solutions to achieve compliance with PCI DSS 4.0 to secure the cardholder ecosystem, including its supply chain. The intended audience for the guide includes enterprise architects, DevOps and SecOps managers, and CISOs. The guide will help you to avoid overspending for a solution that is over- or under-engineered for your needs.

DSS PCI 4.0 Overview

Organizations have less than two years to comply with PCI DSS version 4.0, which seems like a lot of time. However, when considering the budgeting, planning, implementation, testing, and attestation of solutions, the window for meeting the new requirements is a fairly short transition timeline. It has been nearly 20 years since PCI DSS was first announced, and the original 12 requirements remain relatively the same, as do many of its supporting technical controls. The standard needed a significant refresh. The last major update was version 3.0 in 2013, when organizations were required to secure cloud technologies and perform penetration testing.

Version 4.0, set for enforceability on April 1, 2025, is a major update requiring covered entities to invest substantial resources and investment to achieve compliance. Version 4.0 went through three requests for comments and received over 6,000 feedback comments from over 200 companies. By any measure, this release is significant to organizations with six major changes:

- **Customized implementation:** Organizations can choose the best methods and technologies to achieve security objectives if they can demonstrate and document their effectiveness. This change recognizes the need to allow new technology and innovative approaches to compliance.
- **Security as a continuous process:** Organizations must monitor and evaluate their security posture, including their supply chain, on an ongoing basis and perform validation activities at least annually or whenever significant changes occur.
- **Strong authentication and encryption:** Organizations must use stronger and more secure methods for verifying the identity of users, devices, and systems and protecting the confidentiality and integrity of cardholder data, whether in transit or at rest.
- **Secure system components:** Any system components used to process or store cardholder data, including network devices, servers, computing devices, virtual components, cloud components, and software, define the scope of PCI DSS.
- **Advanced and diverse payment fraud detection:** Organizations have to use more advanced and diverse techniques for detecting and preventing fraud, such as tokenization, point-to-point encryption, 3-D Secure, and biometrics.

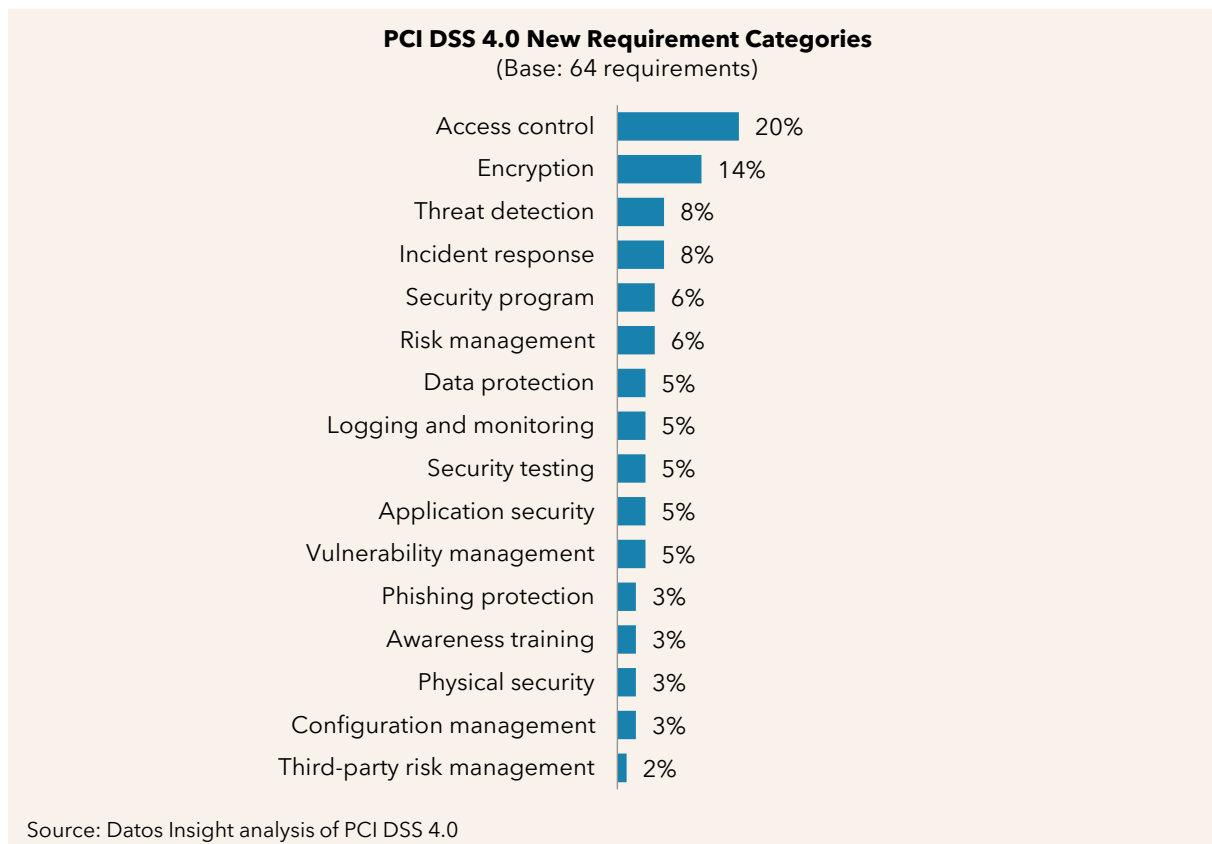
- **Continual compliance:** Compliance activities are no longer considered an annual assessment event. Organizations must continuously assess their security posture and document their control effectiveness.

Versions 3.3.1 and 4.0 are not interchangeable, and compliance must be on one or the other.

What's New in PCI DSS 4.0?

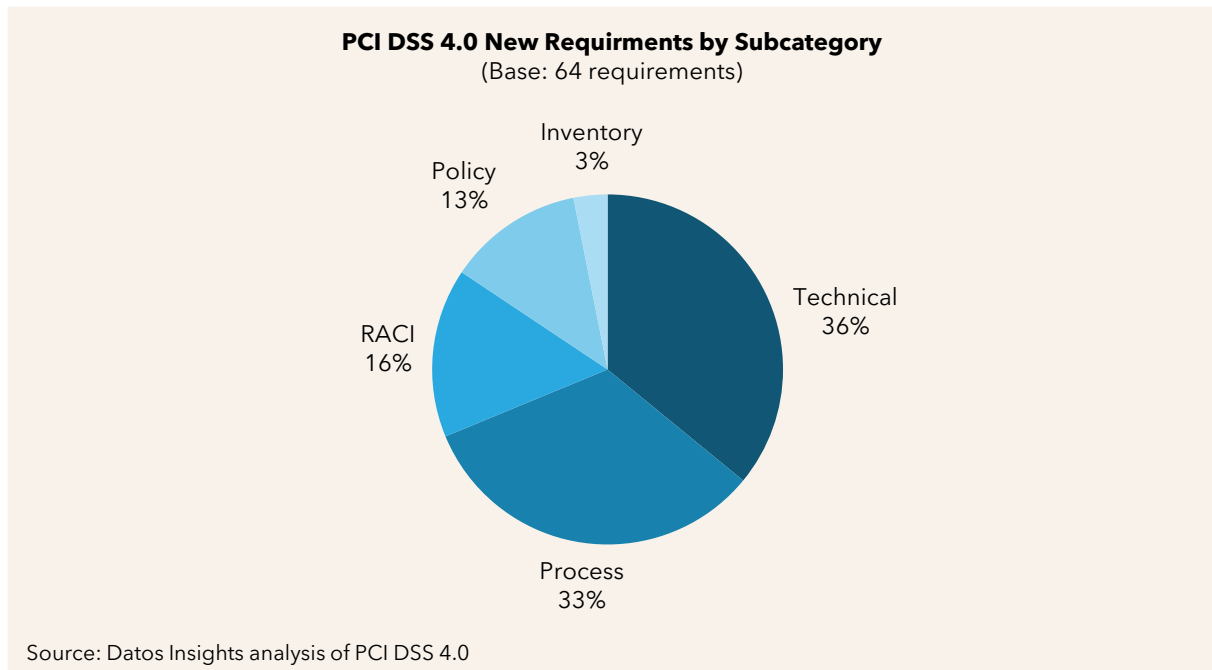
There are 64 new requirements introduced in version 4.0. Various security solutions can address many of these security requirements directly or indirectly. Figure 2 presents the breakdown of PCI DSS 4.0 new requirements by category.

Figure 2: PCI DSS 4.0 New Requirements by Category



Approximately 64% of PCI DSS 4.0 is related to documentation. When applied to system components, the technical subcategories are where security solutions can assist in achieving compliance with the standard.

Figure 3 shows the classification of the new 4.0 requirements by subcategory.

Figure 3: PCI DSS 4.0 New Requirements by Subcategory

New Requirements in Effect Now

Thirteen requirements immediately take effect for organizations declaring to attest to version 4.0. Most requirements are term best practices until their effective date, after which they're simply requirements. Organizations may continue to assess against version 3.2.1 for their assessment due by March 1, 2024, and would not need to complete an assessment against PCI DSS version 4.0 until their annual assessment.

Future-Dated New Requirements

Future-dated requirements fall into two categories. The first category consists of requirements primarily oriented toward people, documentation, and policies. The second category is technology-oriented, relating to changes or new technologies.

Table A presents technology-related future date requirements and recommendations on how to comply with PCI DSS requirements. Readers are encouraged to consult the PCI Council version 4.0 documentation for full explanations of each requirement. Controls applied to meet the requirements of PCI DSS 4.0 must be reassessed periodically to ensure they remain fit for purpose.

Table A: Future Date Technical Requirements

PCI DSS 4.0 requirement	Description	Compliance recommendation
3.3.2	Pre-authorization sensitive authentication data must be stored electronically before completion of authorization.	Apply storage-layer encryption of sensitive data-at-rest within applications, databases, and servers. This server-side encryption is considered a minimum requirement.
3.3.3	Any storage of sensitive authentication data is limited to what is needed for a legitimate issuing business need and is secured. This data is encrypted using strong cryptography.	Consider encrypting sensitive authentication data with a cryptographic key different from that used to encrypt the primary account number (PAN).
3.4.2	When using remote-access technologies, technical controls prevent copying or relocating the PAN for all personnel except those with documented, explicit authorization and a legitimate business need.	Implement role-based access control and encryption to protect PANs from unauthorized access, use, and disclosure. Privilege management should be applied to restrict PAN use by authorized users.
3.5.1.1	Hashes that render PANs unreadable are keyed cryptographic hashes of the entire PAN.	Use data encryption to protect PANs data from unauthorized access. Maintain an inventory of trusted keys and certificates to protect PAN during transmission.
3.5.1.2	If disk- or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PANs unreadable, it is implemented only on removable electronic media. Or, if used for nonremovable electronic media, PAN is also rendered unreadable via another mechanism.	Encrypt sensitive data-at-rest located on servers, applications, and databases, known as client-side encryption. Access to data storage devices does not permit access to the plain-text data.

PCI DSS 4.0 requirement	Description	Compliance recommendation
4.2.1	Strong cryptography and security protocols are implemented to safeguard PAN during transmission over open, public networks. Only trusted keys and certificates are accepted. Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.	Identify all connection points where account data is transmitted or received over open public networks. Consider encrypting PAN over internal networks and establishing new network implementations with encrypted communications.
5.3.3	Anti-malware solution(s) for removable electronic media must perform automatic scans or continual behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	Configure anti-malware software to automatically scan removable media at intervals specified by a risk assessment.
5.4.1	Processes and automated mechanisms shall be in place to detect and protect personnel against phishing attacks.	Apply multiple controls, including domain name system (DNS) filtering, to block access from blacklisted phishing domains, block suspicious file types through email gateway rules, and use email server anti-malware protection technology to perform attachment scanning or sandboxing.
6.4.2	To detect and prevent web-based attacks continually, an automated technical solution must be deployed for public-facing web applications.	Deploy a web application firewall (WAF) or WAAP solution that continuously analyzes inbound web applications and API traffic to identify and block advanced, low, and slow attack tactics. Consider solutions that use behavioral analysis to detect sophisticated attacks, distributed denial-of-service (DDoS) attacks, and Botnet campaigns.

PCI DSS 4.0 requirement	Description	Compliance recommendation
6.4.3	Payment page scripts loaded and executed in the consumer's browser are managed where methods are implemented to confirm that each script is authorized, and its integrity ensured. An inventory of all scripts is maintained with written justification for why each is necessary.	Apply technical controls to protect against client-side computing attacks, including digital signatures and version control. Utilize script management to ensure that only authorized scripts, such as .js and .ts files, can execute. Block unauthorized scripts from executing.
8.3.6	If passwords and passphrases are used, password length shall be at least 12 characters (or if the system does not support 12 characters, a minimum of eight characters).	Enforce unique complex 90-day expiring passwords that comprise a minimum of 12 characters. Use a password manager application that stores and encrypts all user passwords under one master password. Passwordless authentication can also be deployed.
8.4.2	Multi-factor authentication (MFA) is required to access the cardholder data environment.	Implement FIDO-based phishing-resistant MFA, the most secure approach to MFA deployments.
8.5.1	Extension of the PCI DSS MFA system requirements in line with the PCI Security Standards Council MFA guidance. Two different MFA authentication factors must be used.	Deploy an MFA solution immune to replay attacks, cannot be bypassed by users and administrators, enforces independent factors, and all authentication factors must pass.
8.6.1	If accounts used by systems or applications can be used for interactive login, they are managed as follows: Interactive use is prevented unless needed for an exceptional circumstance. Interactive use is limited to the time needed for exceptional circumstances. Business justification for interactive use is documented.	Configure system and application accounts to disallow interactive login to prevent unauthorized individuals from logging in and using the account with its associated system privileges and to limit the machines and devices on which the account can be used.

PCI DSS 4.0 requirement	Description	Compliance recommendation
10.4.1.1	Requires the use of automated mechanisms to perform audit log reviews.	Implement automated log alerting and reviews using a security information and event management solution that provides log harvesting, parsing, and event alerting.
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly.	Require full security device stack observability and alerting on degrading performance or failure. The security system's health, capacity, and performance should be continuously monitored with deviations to the optimum state alerted.
11.3.1.2	Internal vulnerability scans must be performed via authenticated scanning.	Configure internal vulnerability scanning services platforms to use credentials with privileges and sufficient access rights to perform full administrative-level scans.
11.4.7	Multitenant service providers support their customers with external penetration and technical testing by providing access or evidence that comparable technical testing has been undertaken.	Conduct penetration tests to simulate attacker behavior and discover vulnerabilities in their environment. In shared and cloud environments, the multitenant service provider may be concerned about the activities of a penetration tester affecting other customers' systems.
11.5.1.1	Intrusion-detection and intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels. Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel or automated, ensuring such communications are blocked.	Detect covert malware communication attempts (for example, DNS tunneling) to block the spread of malware laterally inside a network and data exfiltration. When deciding where to place this control, entities should consider critical network locations and likely routes for covert channels. When malware establishes a foothold in an infected environment, it often tries to establish a communication channel to a command-and-control server.

PCI DSS 4.0 requirement	Description	Compliance recommendation
11.6.1	A change-and-tamper-detection mechanism must be deployed for payment pages that alert personnel to unauthorized modifications to the HTTP headers and the contents of payment pages.	Deploy client-side protection providing page integrity monitoring that alerts on unauthorized modification, indicators of compromise, page changes, additions, and deletions to the HTTP headers and the contents of payment pages received by the consumer browser.
A1.1.1	The multitenant service provider confirms that access to and from the customer environment is logically separated to prevent unauthorized access.	Ensure strong separation between environments designed for customer access, for example, configuration and billing portals, and the provider's private environment that should only be accessed by authorized provider personnel.
A1.1.4	The multitenant service provider confirms the effectiveness of logical separation controls used to separate customer environments at least once every six months via penetration testing.	Test the effectiveness of logical separation controls used to separate customer environments at least once every six months via penetration testing.
A1.2.3	The multitenant service provider implements processes or mechanisms to report and address suspected or confirmed security incidents and vulnerabilities.	Implement secure methods for customers to report security incidents and vulnerabilities to encourage them to report potential issues and enable the provider to learn about and address potential issues within their environment quickly.
A3.3.1	Failures of the following are detected, alerted, and reported in a timely manner using automated log review mechanisms and automated code review tools.	Detect failures of critical security control systems through detection, alerting, and addressing failures promptly. Systems include IDS/IPS, FIM, anti-malware solutions, physical and logical access controls, and audit logging mechanisms.



Source: Datos Insights analysis of PCI DSS 4.0




Cybersecurity Technologies to Achieve Compliance

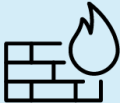
The principal requirement for this version of PCI DSS is the broader range of network security controls versus the focus on firewalls and routers. Adopting the PCI DSS good practices will lessen the load most organizations will face in achieving compliance. Version 4.0's outcome-based approach allows organizations to focus on reducing risk rather than counting controls. Many best and good practices become requirements on April 1, 2025.

Table B summarizes PCI DSS 4.0 recommended good practices that can be generally addressed through commercial cybersecurity solutions.

Table B: PCI DSS Good Practices

Solution category	PCI DSS good practice	Recommendation
 API and bespoke software Requirement 6.3.2	Identifying and listing all bespoke and custom software and any third-party software incorporated into the entity's bespoke and custom software enables the entity to manage vulnerabilities and patches. Vulnerabilities in third-party components (e.g., libraries, APIs) embedded in an entity's software also render those applications vulnerable to attacks.	<p>Deploy an API protection solution to discover, inventory, and remediate vulnerabilities in APIs that process, receive, transmit, and store cardholder data. Include open-source and third-party payment applications, components, and APIs. Access to APIs must also be strictly enforced to authorized users.</p> <p>Inventory of bespoke custom and third-party software components must be maintained to facilitate vulnerability and patch management. Software bill of materials is well suited for this requirement to secure the software supply chain.</p>
 Bot protection Requirement: 6.4.3	Bots are used to perpetrate fraud at an unimaginable scale. Whether scam, click, or DDoS bots, each has a singular goal: to aid cybercriminals in committing fraud.	PCI DSS requires organizations to use more advanced and diverse techniques to detect and prevent fraud, such as tokenization, point-to-point encryption, 3-D Secure, and biometrics. Deploy a bot management solution to prevent browser-based bot attacks.

Solution category	PCI DSS good practice	Recommendation
 Client-side protection Requirements 6.4.3 and 11.6.1	<p>Client-side is a potential avenue for malicious actors to target scripts loading and executing in the payment page where their functionality can be altered without the user's knowledge and can also have the functionality to load additional external scripts.</p>	<p>Allow only authorized scripts where the payment page is loaded into an inline frame, restrict the location where a payment page can be loaded, and use the parent page's content security policy to prevent unauthorized content from substituting for the payment page. Each script is justified as to why it is needed for the functionality of the payment page to accept a payment transaction.</p>
 DDoS attack prevention Requirement: 6.4.2	<p>DDoS attacks are a type of web-based attack designed to overwhelm a web server or application with a large volume of traffic, rendering it unavailable or slow for legitimate users.</p>	<p>Deploy a DDoS prevention solution that provides rate limiting combined with other techniques, such as network design, threat monitoring, filtering of malicious traffic, and scalable DDoS attack traffic absorption provided by edge servers.</p>
 Runtime protection Requirement 6.4.1	<p>A good practice is implementing a runtime application self-protection (RASP) technology. RASP solutions can detect and block anomalous behavior by the software during execution. RASP solutions monitor and block behavior within the application. WAFs typically monitor the application perimeter.</p>	<p>Deploy a RASP solution to detect and block anomalous behavior by software during execution. RASP solutions monitor and block malicious behavior within the application.</p>

Solution category	PCI DSS good practice	Recommendation
 WAF Requirement 6.4.2	A WAF installed in front of public-facing web applications to check all traffic is an example of an automated technical solution that detects and prevents web-based attacks. WAFs filter and block nonessential traffic at the application layer. A properly configured WAF helps to prevent application-layer attacks on applications that are improperly coded or configured.	Deploy a WAF in front of public-facing web applications, inspecting all traffic and serving as an automated technical solution that detects and prevents web-based attacks.

Source: PCI DSS v4 standard

Conclusion

- Complexity in payment cards and the rapidly evolving threat landscape are the principal drivers to having a standard encouraging a continuously improving security posture that instills more rigor in securing payment cardholder data, including its supply chain.
- PCI DSS version 4.0 departs from the previous minor change-oriented releases organizations have grown accustomed to. With 64 new requirements, this transformational release represents a significant effort and investment for many organizations.
- The two versions of PCI DSS are not interchangeable. Organizations must comply with one or the other. The customized validation approach can only be used with version 4.0. Organizations cannot wait to comply with version 4.0 by their next compliance date after March 31, 2025.
- Any system components used to process or store cardholder data, including network devices, servers, computing devices, virtual components, cloud components, and software, define the scope of PCI DSS. Organizations must apply security to the entirety of the attack surface of system components.
- Include solutions and strategies to address the rapidly emerging risk of client-side compromise. Sensitive data must be protected from exposure or theft on the user's browser. Consider encrypting, masking, or tokenizing data before sending it to the web server or application or displaying it on the web page.
- Small to midsize organizations may continue their defined key and compensating control implementation regime. However, risk-mature organizations can adopt an outcome-focused, customized approach supported by a targeted risk analysis, documentation, and proof of control effectiveness.
- Implementing integrated security solutions that incorporate most, if not all, of the PCI DSS requirements is effective and cost-advantaged. Working with security solution providers with a deep understanding and track record of helping organizations comply with the PCI DSS standard is optimal.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives and experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779

Boston, MA 02109

www.datos-insights.com

Author information

Tari Schreider

tschreider@datos-insights.com

© 2024 Datos Insights or its affiliates. All rights reserved. This publication may not be reproduced or distributed in any form without Datos Insights' prior written permission. It consists of information collected by and the opinions of Datos Insights' research organization, which should not be construed as statements of fact. While we endeavor to provide the most accurate information, Datos Insights' recommendations are advisory only, and we disclaim all warranties as to the accuracy, completeness, adequacy, or fitness of such information. Datos Insights does not provide legal or investment advice, and its research should not be construed or used as such. Your access and use of this publication are further governed by Datos Insights' Terms of Use.