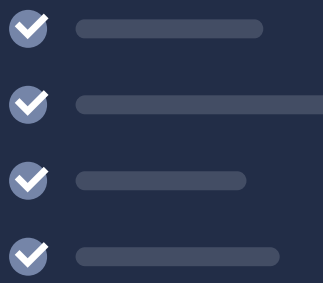
SECURE CODE WARRIOR

Preparing for PCI-DSS 4.0 Compliance

Evaluate your infrastructure and processes to support PCI-DSS requirements



Key updates and timelines for the new PCI-DSS 4.0 requirements

PCI-DSS 4.0 introduces updates to enhance the security of cardholder data, addressing current risks and technological advancements in the payment card industry. The revisions allows organizations to adopt customized security measures if they demonstrate compliance with security objectives, extending multifactor authentication to all access in the cardholder data environment, and strengthening encryption across all networks. Additionally, there is greater emphasis on continuous risk analysis and mitigation, and improving capabilities for timely detection and response to security incidents. These new requirements have a transition period to allow organizations time to adopt the new version while maintaining compliance under the existing standards.

Why CISOs should prioritize the latest pci-dss updates

Adhering to these updated standards is crucial for not only maintaining compliance, but for also protecting against new and emerging cyber threats and risks. By implementing these standards, organizations can be resilient against breaches, thereby protecting their reputations and avoiding potentially hefty fines for non-compliance.

Effective date of DSS 4.0: March 2024; actualized by March 2025

PCI-DSS 4.0 emphasizes the importance of integrating continuous security processes into daily business operations

Compliance can't just be a one-time assessment. This approach is vital for CISOs tasked with fostering a culture of security awareness and proactive risk management within their organizations. Embracing PCI-DSS 4.0 also helps drive business value by building a robust security infrastructure that underpins safe and secure payment environments.

Are your developers prepared to deliver compliant software?

Developers sit as an integral - yet often underutilized - part of reaching a state of software security excellence. It is crucial developers understand the broader picture of PCI DSS 4.0 and what they can control and integrate as part of their default approach to a software build.

Requirement 6 of the PCI DSS outlines expectations for developing and maintaining secure software

This includes a variety of items ranging from secure development standards to developer training to configuration and change control management. Any organizations that develop software used in a Cardholder data network (CHD) are required to comply with these mandates.

As outlined in requirement 6.2.2, software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including how to use the security testing tools for detecting vulnerabilities in software.

The standard further outlines that training should include at least the following items:

- Development languages in use
- Secure software design
- Secure coding techniques
- Use of techniques/methods for finding vulnerabilities in code
- Processes to prevent reintroducing previously resolved vulnerabilities

Additionally, developers should be familiar with ALL of the attack techniques (outlined in Requirement 6.2.4.) This includes a list of attack categories designed to serve as examples:

- Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.
- Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.
- Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.
- Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).
- Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.
- Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

How Secure Code Warrior can help you achieve PCI-DSS 4.0 compliance

The most effective option for training is an agile learning platform where compliance becomes a byproduct of an overarching secure code learning program. Specifically, Secure Code Warrior can help your company reduce vulnerabilities and achieve greater developer productivity by:

Delivering a solid, consistent understanding of how to keep PCI data safe by addressing gaps in knowledge and providing precision training in the languages and frameworks that your developers use. See more on our Learning Platform.

Offering a continuous, measured, and established skills verification process to ensure training has been absorbed and put into practice. Learn more about our ready-made secure code training pathways for developers.

Conducting training via agile learning methods that provide just-in-time, contextual microbursts of learning. Generic, infrequent training is no longer viable, and it won't have the desired impact on vulnerability reduction. Learn more about our supported vulnerabilities.

Aiding in documenting security training and coding standards, useful for demonstrating compliance during PCI-DSS audits. For a more detailed breakdown of PCI-DSS 4.0, check out our whitepaper, PCI DSS 4.0 Unraveled.

About Secure Code Warrior

Secure Code Warrior gives your developers the skills to write secure code. Our learning platform is the most effective secure coding solution because it uses agile learning methods for developers to learn, apply, and retain software security principles. Over 600 enterprises trust Secure Code Warrior to implement agile learning security programs, deliver secure software rapidly, and create a culture of developer-driven security.

Securecodewarrior.com | Request a demo

Find us on Social:

SECURE CODE WARRIOR