PCI DSS: Protecting Payment Card Data

Created and maintained by major players in the payment card industry, the Payment Card Industry Data Security Standard (PCI DSS) aims to ensure that merchants and service providers worldwide securely process, transmit, and store payment card details. If an organization accepts payment cards in any way (in person, by phone, or via the internet), compliance is required.

Organizations covered by the framework must conduct a thorough review of current security measures to avoid penalties, which can reach up to $100,000 per month or result in the loss of ability to process payment cards.

The cornerstone of PCI DSS validation is a set of rigorous annual assessments designed to provide a comprehensive evaluation of the security posture. However, compliance is not one-size-fits-all. Organizations with a higher volume of transactions have more rigorous requirements.

PCI DSS and Penetration Testing Requirements

PCI DSS is highly prescriptive regarding penetration testing obligations. Pentesting is explicitly listed under Requirement 11 of the standard.

- **Mandatory testing:** Companies must conduct external and internal penetration testing at least annually and anytime there is a significant infrastructure or application upgrade or modification (e.g., new system component installations).
- **Scope definition (CDE):** Pentests must cover the entire cardholder data environment (CDE) and all systems and networks connected to it. This includes storage locations, critical network connections, access points, and applications that store, process, or transmit cardholder data.
- **Testing types:** Testing must be conducted both externally (perimeter, using non-authenticated “black box” testing) and from inside the network (internal, with internal accounts and network access). It must include both network-layer and application-layer attacks.
- **Segmentation validation:** PCI DSS requires pentesting to validate that segmentation controls are operational, effective, and isolate all out-of-scope systems from systems in the CDE.
- **Risk ranking:** Requirement 6 highlights the need to establish a process to identify security vulnerabilities and assign a risk ranking, noting that this is not achieved by automated vulnerability scanning (ASV) alone. Pentesting reports from reputable vendors typically include risk ranking.

PCI DSS 4.0: Evolving Security Standards

PCI DSS 4.0 went into effect on April 1, 2024. It marks a significant update, designed to address the evolving threat landscape. Key changes reinforce the need for robust security testing.

1. **Outcome-based approach:** The new standard shifts from highly prescriptive controls to a more flexible, outcome-based approach, allowing organizations to tailor security measures to their unique risk profile.
2. **Continuous monitoring:** PCI DSS 4.0 emphasizes continuous security monitoring, detection, and response, encouraging organizations to address advanced persistent threats (APTs) and insider risks, rather than overstressing prevention alone.
3. **Rigor in testing:** The standard requires stricter testing and validation procedures, explicitly mentioning penetration testing, vulnerability scanning, and application security assessments to prove the effectiveness of controls.

Tiered Approach: Requirements Across PCI Compliance Levels

PCI DSS compliance uses a tiered approach, with four levels, based on a merchant's annual payment card transaction volume. A critical requirement for all four levels is the mandatory quarterly network vulnerability scan, which must be performed by an Approved Scanning Vendor (ASV).

- **Level 1:** This is the highest tier, for merchants processing over 6 million transactions annually. Compliance must be validated through a formal, on-site audit conducted by an independent Qualified Security Assessor (QSA). This audit results in a detailed Report on Compliance (ROC) and a summary Attestation of Compliance (AOC).
- **Levels 2, 3, and 4:** These lower tiers, for merchants with smaller transaction volumes, do not require a formal QSA-led audit. Instead, they use a Self-Assessment Questionnaire (SAQ) to self-validate their compliance.

Frequency of Testing

PCI DSS mandates a testing schedule with varying frequencies based on the type of test and the entity involved.

- **Semi-annually:** Multi-tenant service providers must validate their logical network segmentation controls every six months to ensure client environments remain isolated.
- **Quarterly:** All organizations must conduct external vulnerability scans with an ASV. They must also perform internal vulnerability scans and scans for rogue wireless access points quarterly (every 90 days).
- **Event-driven:** Pentesting and vulnerability scanning are mandated not only on a fixed schedule but also after any "significant change" to the environment. This includes events like new system installations, major upgrades, or changes to network topology.

These mandates for quarterly vulnerability scans, and event-driven pentesting after any significant system change, mean that security validation must be an ongoing process, ensuring that new vulnerabilities are identified and addressed promptly to maintain compliance throughout the year.

See how Cobalt helps Insurity comply with PCI DSS

READ CASE STUDY

About Cobalt

Cobalt is the pioneer in pentesting as a service (PTaaS) and a leader in offensive security services.

We are focused on combining talent and technology with speed, scalability, and expertise. Thousands of customers and hundreds of partners rely on the Cobalt Offensive Security Platform, along with the industry's largest exclusive community of 450+ trusted pentesters and security experts, to find and fix vulnerabilities across their environments. By enabling faster pentest launches, real-time collaboration with testers, continuous scanning, and seamless integration with remediation workflows, we help organizations identify critical issues and accelerate risk mitigation so they can operate fearlessly and innovate securely.

Book a demo to see how Cobalt can help you achieve compliance and build your offensive security program.

BOOK A DEMO