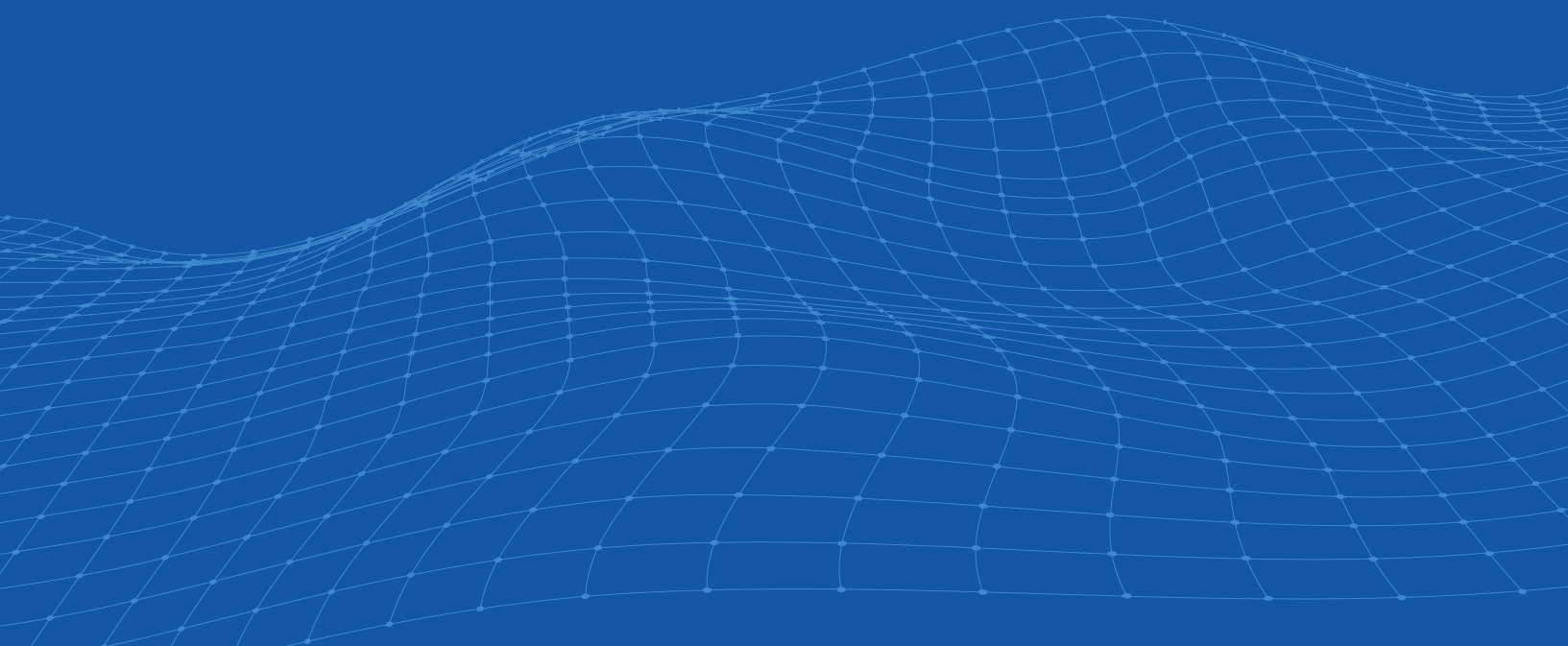
Cobalt

WHITE PAPER

Compliance-Driven Penetration Testing

A Guide to Major Data Security Frameworks



Contents

Introduction and Overview 3

PCI DSS: Protecting Payment Card Data 5

HIPAA: Securing Electronic Protected Health Information 8

SOC 2: Demonstrating Trust in Service Organizations 9

ISO 27001: Proving Information Security Management Resilience 10

European Cyber Resilience Act (CRA): Overview and Compliance Best Practices 11

From Compliance-Driven Testing to Programmatic Security 13

About Cobalt 14

Introduction and Overview

Compliance frameworks, while sometimes viewed as a hurdle, are essential for establishing a robust and effective security program. For many organizations, a compliance obligation is the most common trigger for a penetration test (pentest). Adherence to these standards, such as PCI DSS, HIPAA, SOC 2, and ISO 27001, is often a prerequisite for business engagements, accelerating sales cycles, reducing due diligence times, and fostering trust with customers and partners.

How Penetration Testing Drives Compliance

Penetration testing plays a crucial role in meeting and exceeding regulatory requirements by providing third-party validation and practical evidence of a strong security posture.

1. **Validating controls and identifying risks:** Pentesting simulates real-world attacks to uncover security weaknesses in systems, networks, and applications. It assesses the effectiveness of existing security controls in preventing and mitigating potential attacks. Compared to automated scanners, manual pentesting is better suited to finding complex vulnerabilities, such as business logic flaws or chained exploits.
2. **Meeting specific mandates:** Some frameworks, like PCI DSS, explicitly mandate regular pentesting. For others, like SOC 2 and proposed HIPAA updates, pentesting is a necessary independent evaluation or required control.
3. **Demonstrating continuous improvement:** Achieving compliance is not a one-time event; it requires continuous monitoring, testing, and improvement. A formalized pentest program can provide consistent data, highlight performance trends, and demonstrate improvements in control maturity over time.
4. **Audit readiness:** Pentesting produces audit-quality attestation reports that serve as a key artifact for demonstrating due diligence to auditors and regulatory authorities.

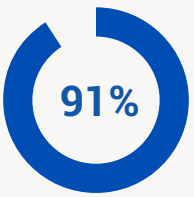
Crucially, implementing a well-rounded pentesting approach allows organizations to meet the requirements of multiple compliance frameworks simultaneously. It is also seen by many security professionals as a key element of their security program, customer trust, and the success of their business.

According to the 2025 State of Pentesting Report from Cobalt, 91% of security leaders and practitioners believe pentesting is critical for meeting business and compliance goals, while 94% state pentesting is “foundational” for modern security programs.

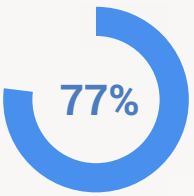
Top Reasons Organizations Perform Pentesting

Foundational for modern programs to ensure a strong security posture

Important to our organization’s strategy and senior leadership



Critical for meeting our business and compliance goals



Improves customer trust in our software products

Figure 1. Results from a survey of 500 security leaders and practitioners. Source: State of Pentesting Report 2025.

Compliance Standards Overview

The table below summarizes the four major compliance frameworks and their reliance on pentesting.

Framework	Requirement	Pentesting Role	Key Facts
PCI DSS Payment Card Industry Data Security Standard	Required for any company that processes, transmits, or stores payment card data	• Mandatory annual internal and external pentesting of the Cardholder Data Environment (CDE) • Additional testing required after significant changes to the environment	• PCI DSS 4.0 mandates more rigorous testing and validation procedures and emphasizes continuous security monitoring • Non-compliance can result in penalties up to $100,000 per month or loss of ability to process payment cards
HIPAA Health Insurance Portability and Accountability Act	Required for US companies handling sensitive patient health information (e-PHI)	• Pentesting is part of the security rule's requirement for risk assessments and security measure evaluation. • Proposed updates for 2026 mandate annual pentesting	• Focuses on protecting the confidentiality, integrity, and availability of e-PHI • Mandates implementing security measures that are reasonable and appropriate
SOC 2 System and Organization Controls 2	Voluntary, but often required by security-conscious partners and clients, especially for SaaS/cloud providers	• Explicitly mentions pentesting under CC4.1 COSO Principle 16 • Pentesting acts as an independent evaluation to ensure the effectiveness of internal controls	• Demonstrates a commitment to protecting customer data security, availability, processing integrity, confidentiality, and privacy • The resulting report is a key auditor artifact
ISO 27001 Information Security Management System	Voluntary global standard, popular internationally	• Pentesting strengthens required controls (A12.6: Technical Vulnerability Management and A14.1.2: Securing Application Services) • Supports the core requirement to discover, evaluate, and handle risks	• Following this comprehensive framework establishes a robust security program • Regular pentests demonstrate corrective actions and maturation of security controls over time
EU CRA European Union Cyber Resilience Act	Required for manufacturers, importers, and distributors of products with digital elements (PDEs) sold in the EU	• Manufacturers must conduct continuous risk assessments and ensure products are released without exploitable vulnerabilities, making penetration testing a critical compliance tool	• Compliance is a prerequisite for the CE mark (Conformité Européenne), mandatory for products sold in the European Economic Area (EEA) • Non-compliance can lead to fines up to €15M or 2.5% of global turnover, and product recalls

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.

HIPAA: Securing Electronic Protected Health Information

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law established to protect sensitive patient health information. If a company provides medical services in the U.S. or works in partnership with U.S. medical providers, compliance with HIPAA recommendations is mandatory. The framework aims to secure electronic protected health information (e-PHI).

Pentesting as a Security and Risk Analysis Tool

The HIPAA Security Rule requires organizations to implement security measures that are "reasonable and appropriate" for their specific entity. While this language historically allowed for considerable discretion, penetration testing fulfills essential components of the rule.

- **Risk analysis and assessment:** HIPAA requires a risk analysis that includes evaluating the likelihood and impact of potential risks and reviewing and considering threats and vulnerabilities experienced in the last 12 months. Pentesting provides an in-depth review of discovered vulnerabilities and helps organizations document their approach to assessing and addressing the risk posed by exploitable vulnerabilities.
- **Periodic assessment:** Pentesting can fulfill the requirement for a periodic assessment of whether security policies meet the rule's requirements, providing a thorough analysis from an impartial third party.
- **Scope:** Security controls should focus specifically on defending electronic protected health information.

Stricter Requirements Going Into Effect in 2026

Recent proposed updates to HIPAA security regulations are tightening security guidelines and clarifying that all security guidelines are mandatory. Although the proposed changes are not final as of Q4 2025, it is likely they will not change significantly before final implementation sometime in 2026. These changes integrate the concept of Cybersecurity Performance Goals (CPGs) into the regulatory framework.

The enhanced goals include establishing pentesting and attack simulation processes. Most notably, the proposed security rule would explicitly require organizations to implement semi-annual vulnerability scanning and annual pentesting.

These new requirements underscore the transformation of pentesting from a highly recommended practice to a mandatory, auditable control for organizations handling e-PHI. By proactively protecting against breaches involving e-PHI, through a rigorous security testing program, organizations minimize HIPAA compliance risk and ensure patient trust.

SOC 2: Demonstrating Trust in Service Organizations

SOC 2 (System and Organization Controls) is a framework developed and maintained by the American Institute of Certified Public Accountants (AICPA). The framework establishes controls designed to help service organizations protect the security, availability, processing integrity, confidentiality, and privacy of sensitive information.

SOC 2 Compliance and Pentesting

While SOC 2 is a voluntary framework and never a legal requirement, certification has become widely regarded as proof that a company has taken appropriate measures to protect customer data. Many security-conscious companies, especially those providing cloud or Software-as-a-Service (SaaS), require SOC 2 compliance from their partners' accountants.

SOC 2 requires companies to have a formal process to identify, track, and resolve security vulnerabilities. Pentesting plays a vital role in validating this process:

- **Independent evaluation:** SOC 2 specifically mentions pentesting under CC4.1 COSO Principle 16, which states that management should use "a variety of different types of ongoing and separate evaluations, including penetration testing ... and internal audit assessments."
- **Key audit artifact:** A pentest report is considered a key artifact for demonstrating due diligence to auditors, proving that process controls are rigorously tested.
- **Comprehensive findings:** Since compliance requires identifying security vulnerabilities, manual pentesting is essential for discovering more complex issues, such as business logic or chained exploits, that automated scanners typically miss.

Type I vs. Type II Audits

When pursuing SOC 2 compliance, organizations must choose between a Type I and a Type II audit, which determines how controls are evaluated:

- **SOC 2 Type I Audit:** Attests to the design and implementation of controls at a single point in time.
- **SOC 2 Type II Audit:** Attests to the design, implementation, and operating effectiveness of controls over a period of time, usually three to 12 months.

A Type II audit generally provides a greater level of trust to customers because it verifies that controls operated effectively over a duration. Integrating continuous pentesting into the development lifecycle ensures organizations maintain the strong compliance posture needed to satisfy the scrutiny of a Type II audit.

ISO 27001: Proving Information Security Management Resilience

ISO 27001 is a voluntary international standard that outlines a set of best-practice guidelines for implementing an Information Security Management System (ISMS). The framework helps businesses protect the security of assets such as financial information, intellectual property, and customer data. While voluntary, ISO 27001 is popular globally, and many international organizations require partners and contractors to be certified.

Pentesting in Support of the ISMS

A core component of ISO 27001 is defining an organization's risk appetite and posture and developing a plan to discover, evaluate, and handle risks. Pentesting directly supports these objectives and ensures the resilience of the ISMS.

- **Vulnerability management:** Pentesting reinforces ISO 27001's control A12.6 (Technical Vulnerability Management), which requires organizations to collect information on technical vulnerabilities in a timely fashion, use it to evaluate cyber risk, and take appropriate measures to address it.
- **Securing public networks:** Pentesting helps fulfill A14.1.2 (Securing Application Services on Public Networks), which mandates protecting services accessible via public networks from security threats.
- **Risk discovery:** Manual pentesting excels where vulnerability scanning tools fall short, identifying complex, business logic-related, and chained vulnerabilities that are critical for accurate risk evaluation.
- **Demonstrating maturity:** The framework requires organizations to demonstrate corrective actions and improvements in control maturity over time. Regular pentesting provides the evidence needed to show continuous detection and remediation guidance, thereby strengthening security controls.

By aligning pentesting efforts with ISO 27001 requirements, organizations can establish robust security programs and prove their commitment to information security for international partners.

European Cyber Resilience Act (CRA): Overview and Compliance Best Practices

The European Cyber Resilience Act (CRA) is a new legal framework adopted by the European Council in late 2024. It introduces mandatory cybersecurity requirements for products with digital elements (PDEs)—both hardware and software—sold in the European Union market.

The regulation aims to ensure that manufacturers, importers, and distributors prioritize security throughout a product's entire lifecycle. By establishing universal standards, the CRA seeks to close supply chain vulnerabilities and empower consumers to identify and select secure products.

Who Is Impacted?

The CRA applies to the entire supply chain of connected devices sold in the EU, regardless of where the company is headquartered.

- **Manufacturers:** Must ensure products are designed, developed, and produced with security in mind. They are responsible for risk assessments, vulnerability handling, and documentation (including software bill of materials—SBOMs).
- **Importers and distributors:** Must verify that products bear the CE conformity marking and that the manufacturer has met all technical documentation and conformity assessment requirements.

What's Covered: Products with Digital Elements (PDEs)

The regulation covers almost all connected hardware and software, including:

- **Consumer tech:** Smartphones, laptops, smart speakers, and connected home appliances.
- **Software:** Operating systems, word processors, and games.
- **Infrastructure:** Firewalls, VPNs, and intrusion detection systems.
  (Note: Medical devices, aviation equipment, and connected cars are excluded as they are covered by existing specific legislation.)

Penalties

Non-compliance with the CRA can result in significant fines (up to €15 million or 2.5% of global turnover) and product withdrawals.

Key Compliance Requirements

To obtain the CE mark required to sell in the EU, organizations must demonstrate the following:

1. **Security by design:** Integrate cybersecurity into the design, development, and production phases.
2. **Vulnerability management:** Detect and mitigate vulnerabilities for a support period of five years (or the product's expected lifetime).
3. **Transparency:** Provide a Software Bill of Materials (SBOM) and technical documentation.
4. **Reporting:** Actively report exploited vulnerabilities and incidents to relevant authorities.

Implementation Timeline

- **Reporting obligations begin September 11, 2026:** Manufacturers will be required to report actively exploited vulnerabilities and severe incidents to authorities (ENISA and national CSIRTs) starting on this date.
- **Full implementation and enforcement begins December 11, 2027:** By this date, all products sold in the EU market must be fully compliant with all CRA requirements, including CE marking, technical documentation, and security support lifecycles.

How Penetration Testing Supports CRA Compliance

The CRA explicitly requires manufacturers to conduct ongoing risk assessments and ensure products are released without exploitable vulnerabilities. Penetration testing is a critical tool for meeting these obligations.

- **Map the attack surface:** Offensive security testing helps manufacturers identify all digital elements and entry points, a prerequisite for the required risk assessments.
- **Identify and mitigate vulnerabilities:** Regular pentesting validates that products are free of known exploitable vulnerabilities before they hit the market—a core CRA mandate.
- **Continuous support:** The CRA requires vulnerability management for five years after release. Continuous pentesting ensures emerging threats are identified and mitigated throughout this support lifecycle.
- **Audit-ready documentation:** Professional pentest reports serve as audit-quality evidence of due diligence, supporting the technical documentation required for conformity assessments.

Establishing a robust offensive security program now allows organizations to map their risks, secure their supply chain, and prepare for the reporting deadlines ahead.

From Compliance-Driven Testing to Programmatic Security

For many organizations, meeting compliance requirements is a primary driver of security activities. Successfully passing these audits is a critical business function that effectively reduces compliance risk. While this serves as a foundation, organizations can strategically build upon it by viewing compliance as the floor, not the ceiling, for their security posture.

A programmatic approach to offensive security, featuring more regular pentesting, complements these compliance efforts by addressing the dynamic, real-world threats that emerge between audits. By adopting this continuous improvement cycle, companies not only satisfy auditors but also achieve genuine risk reduction, protect brand reputation, and build deeper customer trust. A more proactive stance transforms security from a cost center into a competitive advantage, demonstrating a commitment to protection that goes beyond the checklist.

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

BOOK A DEMO

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.

Disclaimer: This content provides general information, not legal advice. Cobalt is not responsible for any errors or omissions, and this content does not create an attorney-client relationship. You should always consult a legal professional for advice specific to your situation.

© 2026 Cobalt Labs, Inc. All Rights Reserved.