Beginner’s Guide to Compliance-Driven Pentesting

Cobalt

Contents

Introduction

Let’s start with the elephant in the room: compliance and control frameworks aren’t the most exciting topic.

The lists of required security controls span endless documents, implementation sounds easier than it actually is, and the challenges can be overwhelming for teams that pursue their first certification.

Which is exactly why we pulled together this document, focusing on a specific security control that many teams aren’t sure how to handle — penetration testing. Or, as we call it at Cobalt, pentesting.

A compliance obligation is in fact the most common trigger for a pentest, bringing up questions like “How will pentesting help us get SOC 2 certified?” or “What assets should we pentest for ISO 27001? And how often?” This PDF can answer these questions and guide less experienced teams through the process — regardless if they’re a Cobalt customer or not.

In this document you’ll learn:

✓ The most commonly pursued compliance frameworks, and how they might apply to your business model or objectives;

✓ Where pentesting comes in — either as a requirement, or an extra step that can strengthen other security controls;

✓ What assets to cover in your pentests and the industry-standard methodologies you should be aware of;

✓ How often to pentest and how to organize your program for both short- and long-term wins;

Common Compliance Frameworks

Before we dive into the specifics of pentesting for compliance, we'll go over the basics of the frameworks covered in this document — NIST 800-53, ISO 27001, SOC 2, PCI-DSS and HIPAA. We have chosen these five for a few reasons: they're one of the most commonly followed frameworks; the list makes this document helpful to both US-based and international businesses; and many of their security controls — particularly where pentesting comes in — overlap.

There are likely others that apply to your industry, so we implore you to not take this document as the sole source of truth for your company's compliance obligations. Instead, its contents aim to be informative and guide your pentesting roadmaps, addressing the questions we've most frequently received from our own customers.

Without further ado, let's go over the basics.

NIST 800-53

Required for US federal agencies and businesses that serve them

The National Institute for Standards and Technology (NIST) 800-53 is a comprehensive set of security controls and assessment procedures designed for federal informational systems and organizations. It is a requirement for all US federal government agencies and the businesses that service them — and yet, many more organizations choose to follow the framework.

That's because it's the most comprehensive option. Following the framework is a sure way to establish a robust and effective security program, so we recommend every team to study its catalog of controls.

ISO 27001

Voluntary, demonstrates commitment to appropriate security for information assets

The International Organization for Standardization's (ISO) 27001 framework outlines a set of best-practice guidelines businesses can use to protect the security of assets such as financial information, intellectual property, and customer data. The framework sets out the basis for a broad program that covers all aspects of cybersecurity.

ISO 27001 is a voluntary standard. However, the framework is popular globally, and many international organizations require contractors and partners to be ISO 27001 certified. If your company has a presence outside the US or aims to do business with non-US companies, you may want to earn a certification.

SOC 2

Voluntary, demonstrates commitment to appropriate customer data protection

SOC 2 — which stands for System and Organization Controls — is developed and maintained by the American Institute of Certified Public Accountants (AICPA). The framework lays out a set of controls designed to help service organizations protect the security, availability, processing integrity, confidentiality, and privacy of sensitive information. SOC 2 is a voluntary framework and never a legal requirement.

SOC 2 certification has become widely regarded as proof that a company has taken appropriate measures to protect customer data. Many security-conscious companies require compliance from their partners and suppliers, particularly those that provide cloud services or Software-as-a-Service (SaaS). If your company manages or hosts data on behalf of customers, maintaining SOC 2 compliance can be an integral part of your security, sales and operations workflows.

PCI-DSS

Required for companies handling payment card data

The Payment Card Industry Data Security Standard (PCI-DSS) is arguably the most influential — and certainly the most far-reaching — cybersecurity framework developed. Created and maintained by the biggest players in the payment card industry, the framework aims to ensure that merchants and service providers worldwide process, transmit, and store payment card details securely.

If your company accepts payment cards in any way — in-person, by phone, or via the Internet — you must be PCI-DSS certified.

HIPAA

Required for US companies handling sensitive patient health information

The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that prompted the development of national standards to protect sensitive patient health information. It aims to protect patients' "electronic protected health information" (e-PHI). If your company provides medical services in the US or works in partnership with one or more US medical providers, you must comply with HIPAA recommendations.

Do I Need to Pentest for These Frameworks?

Depending on which frameworks apply to your business, your pentesting obligations will vary. While some are very prescriptive, others are deliberately vague.

In practice, all the frameworks we have covered include a security control that either requires pentesting, or can be strengthened by it. Let's dive into specific examples:

NIST 800-53

Penetration testing can fall under two sections of NIST 800-53:

- ✓ CA-2 — Security Assessments

This control requires an assessment plan that can evaluate how effective the implementation of other security controls is. To be compliant, you need to have independent teams or individuals impartially evaluate your information systems.

But what exactly are these other security controls?

One example is control RA-5. While the body of RA-5 focuses on vulnerability scanning tools, it also notes the importance of manual security testing. Notably, the control requires organizations to implement vulnerability scanning techniques that include standards for "Enumerating platforms, software flaws, and improper configurations" — something that pentesting is far more suited to than an automated scanner.

Under the supplemental guidance, RA-5 also mentions the value of red team exercises — another manual security exercise that follows a similar process to pentesting.

SIDENOTE

The RA-5 control requires companies to conduct vulnerability scanning through a variety of techniques and tools. You can find more info here.

- ✓ CA-8 — Penetration Testing

This control in particular covers pentesting of hardware, software, or firmware components. The goal is to have an independent body determine how resistant your systems are to an attack, and provide an in-depth review of any discovered vulnerabilities.

ISO 27001

Two ISO 27001 controls relate to pentesting:

- ✓ A12.6 — Technical Vulnerability Management

This control mandates that organizations collect information on technical vulnerabilities in a 'timely fashion,' use it to evaluate cyber risk, and take appropriate measures to address it.

- ✓ A 14.1.2 — Securing Application Services on Public Networks

This control requires companies to protect services accessible via public networks (i.e., the Internet) and subject to network-related security threats, such as fraudulent activity and unauthorized disclosure and modification. Companies need to conduct detailed risk assessments and implement secure authentication methods.

Strictly speaking, ISO 27001 doesn't mandate that you follow every control — a major component of this framework is defining your own risk appetite and posture, and defining the controls that are applicable to your organization. You must, however, have a plan in place on how you will discover, evaluate and handle risks. Moreover, the framework's Clause 10 requires that you be able to demonstrate corrective actions and improvements in control maturity over time.

This can apply to application and network vulnerabilities. Traditional network vulnerability scanning tools are good at identifying missing patches and basic misconfiguration issues. However, automated vulnerability scanners usually aren't able to find more complex, business logic-related, and 'chained' vulnerabilities. This is where manual pentesting can step in.

SOC 2

SOC 2 compliance requires companies to have a formal process to identify, track, and resolve security vulnerabilities. While that might sound vague, there is additional information provided under CC4.1 COSO Principle 16, which specifically mentions pentesting:

> **"Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments."**

The point is that companies should establish different types of ongoing and separate evaluations to ensure that their internal controls are effective.

PCI-DSS

PCI-DSS is among the most prescriptive cybersecurity frameworks when it comes to pentesting. Guidelines list it in several places, most notably under two requirements:

- ✓ **Requirement 6 – Develop and Maintain Secure Systems and Applications**

This requirement prompts organizations to: "Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking [...] to newly discovered security vulnerabilities."

The requirement goes on to note that this risk ranking process "is not achieved by an ASV (Approved Scanning Vendor) scan or internal vulnerability scan," and instead requires a dedicated process. Most reputable penetration testing providers include risk ranking in their reports. However, you should check that your chosen vendor's approach is in line with yours.

✓ Requirement 11.4 – **External and Internal Penetration Testing Is Regularly Performed, and Exploitable Vulnerabilities and Security Weaknesses Are Corrected**

To fulfill this requirement, companies must:

- Follow an industry-accepted approach
- Cover the entire cardholder data environment (CDE) — more on this under "What Should I Pentest"
- Test both externally and from inside the network
- Include both network-layer and application-layer attacks
- Review and consider threats and vulnerabilities experienced in the last 12 months
- Document their approach to assessing and addressing the risk posed by exploitable vulnerabilities found during the pentest
- Keep documentation of pentest results and remediation activities for at least 12 months

Since PCI-DSS is such an influential and far-reaching framework, most pentest providers offer a service explicitly based on its requirements.

HIPAA

The HIPAA Security Rule includes requirements for risk assessments, vulnerability management, and technical and administrative safeguards. The rule states that organizations must implement security measures that are 'reasonable and appropriate for a particular covered entity,' and goes on to list the following points on what steps a risk analysis should include:

1. Evaluate the likelihood and impact of potential risks to patient information
2. Implement appropriate security measures to address those risks
3. Document the security measures and their rationale
4. Maintain continuous, reasonable, and appropriate security protections

The framework lists numerous other security controls, one of which is a periodic assessment whether security policies meet the rule's requirements. Pentesting can fulfill this point, providing a thorough analysis from an impartial third party.

TL;DR

Regardless of which framework you're pursuing, pentesting will either help you fulfill a control that specifically calls for it, or bolster other required activities. What's more, one pentesting roadmap brings you closer to compliance with multiple frameworks — you might be preparing for a SOC 2 audit now, but you're also winning points for ISO 27001 further down the line. Overall, it's good practice.

	Controls pentesting fulfills or supports	How
NIST 800-53	CA-2: Security Assessments	An independent body tests how resistant your systems are to an attack and provides an in-depth review of discovered vulnerabilities.
	CA-8: Penetration Testing	
ISO 27001	ISO 27001 Annex: A.12.6 Technical Vulnerability Management	Pentest providers suggest appropriate remediation and can validate fixes with retesting.
	ISO 27001 Annex: A.14.1.2 Securing Application Services on Public Networks	Compared to scanners, pentesting can discover more complex vulnerabilities such as business logic or chained exploits.
SOC 2	CC4.1 COSO Principle 16	Pentesting can be an independent evaluation to ensure the effectiveness of internal controls.
PCI-DSS	Requirement 6.1: Develop and Maintain Secure Systems and Applications	Pentest reports can risk rank vulnerabilities and highlight high criticality findings.
	Requirement 11.3: Implement a Methodology For Penetration Testing	Pentesting can identify vulnerabilities within the entire CDE and the systems maintaining it, and validate segmentation controls meant to isolate the CDE from out-of-scope assets. *
HIPAA	Risk Analysis and Management	Pentest programs can provide a periodic assessment of security protections.

* Unique to pentesting for PCI-DSS. All other items under "How" can combine and apply to each of the other compliance frameworks.

What Should I Pentest?

The frameworks that apply to your business should determine which systems and assets you pentest. Where some — notably, PCI-DSS — are highly prescriptive, most aren't. Instead, each company is left to determine which systems are most appropriate for pentesting and which can be limited to automated scanning solutions. We'll go over the specifics of PCI-DSS and give you some examples of where you can start with the other frameworks.

PCI-DSS

The PCI-DSS framework is explicit about what must be pentested to achieve compliance — the cardholder data environment (CDE) and all systems and networks connected to it. This can include:

- Storage locations of cardholder data.
- Applications that store, process, or transmit cardholder data.
- Critical network connections.
- Access points.

Companies have to pentest the entire CDE both externally (perimeter) and internally. External perimeter testing is conducted using non-authenticated "black box" testing where only external facing IPs and domains are shared with the testers. Internal pentests are conducted by giving testers internal accounts and network access in order to test inside the perimeter.

PCI-DSS also requires pentesting of assets used to maintain systems in the CDE or access cardholder data. This is because compromises in these systems could ultimately lead to a breach of cardholder data.

In practice, many businesses work to identify the scope of their CDE and ensure its components are kept separate from the rest of their IT systems. This minimizes their legal obligation for pentesting and ensures that security issues outside their CDE won't lead to a compromise of cardholder data.

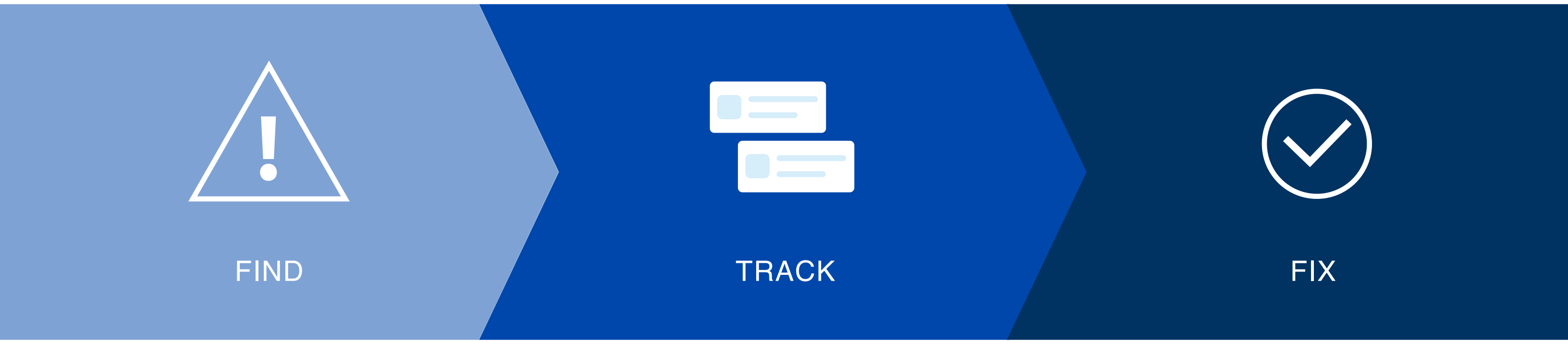
This process is actively encouraged by the PCI-DSS framework, which requires pentesting to “validate that segmentation controls and methods are operational, effective, and isolate all out-of-scope systems from systems in the CDE.”

Other Frameworks

So, what about NIST 800-53, ISO 27001, SOC 2 and HIPAA?

Each of these frameworks gives us much more freedom to decide on the structure of our security assessments. Rather than list precise steps, they offer guidelines that you can use to build the optimal security program, fit to your needs. The only exception is HIPAA, which states that controls should focus on defending electronic protected health information (e-PHI), but is otherwise flexible on how you implement solutions.

There is, however, one trend that runs through all cybersecurity frameworks: the need to find, track, and fix security vulnerabilities.



For most, pentesting every asset, application, and system would be prohibitively expensive. Instead, you should determine which systems are critical to your operations and hold sensitive information. For these assets you can employ a combination of manual pentesting and automated scanning, while other, less critical systems can be covered by automated internal testing.

How Often Should I Pentest?

Of the five cybersecurity compliance frameworks discussed in this ebook, only one provides a specific requirement.

For PCI-DSS compliance, you need to have your CDE pentested “[…] at least annually and anytime there is a significant infrastructure or application upgrade or modification (for example, new system component installations, addition of a sub-network, or addition of a web server).”

NIST 800-53, ISO 27001, SOC 2, and HIPAA all include generic requirements that prompt companies to align pentesting efforts with their business model and environment. For example, by scheduling pentests after major infrastructure changes or when reputable outside sources report on new vulnerabilities.

The challenge is that there is no set-in-stone definition of a ‘major infrastructure change’ and new vulnerabilities can crop up every day. Clearly, no one can hope to pentest every time this happens. And equally, what is considered a ‘major infrastructure change’ for one company could be a routine occurrence for another. Meanwhile, ISO 27001 provides no specific recommendations for pentest frequency, other than that they fit into a continuous vulnerability management program that can demonstrate your controls have matured over time.

Where does this leave us? After assessing their compliance obligations, many opt to pentest just once per year. We believe this is the wrong approach, for two reasons.

First, one-off pentests separated by a full year can rarely (if ever) link up to provide consistent data, highlight performance trends, or inform secure development. Your pentest vendor will complete each test as though it were the first, with no real lessons learned from previous pentests. With no consistent data to work from, the same types of vulnerabilities will likely be reintroduced into your assets and networks over and over again.

Second, security is now a differentiator for many potential customers, or at least a requirement for doing business. As mentioned earlier in this document, they can require partners and suppliers to comply with specific cybersecurity frameworks — often SOC 2 or ISO 27001. Being able to prove a commitment to ongoing security through regular pentest reports can set your business apart from competitors.

So, how often should you pentest? Now it's our turn to be intentionally vague.

The fact is there's no 'ideal' pentest cadence that makes sense for everyone. Your optimal pentest frequency could vary significantly depending on your business's size, function, and objectives.

There are, however, a few rules we can suggest. You should pentest critical systems and assets as frequently as:

1. Makes sense based on how often they undergo changes that can introduce high risk vulnerabilities;
2. Is in line with customer demands or expectations, and;
3. Fits with your security budget and objectives.

If your assets include software developed internally (and particularly if you offer software or cloud products), there's one more thing to keep in mind: security should never happen in isolation. When it comes to product security, all pentesting must be conducted in sync with your product/engineering teams and take place at a cadence that fits the Software Development Lifecycle (SDLC) at your business.

At Cobalt, we've decided on a quarterly testing cadence for key assets, which include the Cobalt web application, API, network and cloud configuration. In the event of larger changes to these components, we perform additional pentests. We do this to ensure that our infrastructure stays secure throughout frequent code pushes, maintain SOC 2 and ISO 27001 compliance, and demonstrate that our platform is secure and trustworthy.

In fact, we pull all of this together in a formalized pentest program — a series of pentests that happen on a regular basis. With a renewable testing cycle, we have continuous coverage for critical assets and can compound data from findings to see long-term security and performance trends.

Key Takeaways

1 One pentesting roadmap has the potential to win you points for multiple frameworks. While PCI-DSS has very specific requirements on how you scope and execute your pentests, consistent and regular pentesting can strengthen your security programs and bring you closer to multiple key certifications.

2 There are multiple well regarded methodologies you can refer to when setting up your first pentest. For networks, you can rely on the Open Source Security Testing Methodology Manual (OSSTMM) and Center for Internet Security (CIS) Controls, while the OWASP Top 10 application security risks are a great place to start for your applications and APIs. A reputable pentest provider will follow these guidelines.

3 Annual pentesting may be enough for compliance, but it’s unlikely to be the best option. Your business should set a pentest cadence based on security needs, customer expectations, and business objectives.

4 A formalized pentest program can help you consistently meet compliance obligations, and gradually mature your security programs.
A series of regular pentests can inform secure development, provide performance data and guide strategic decisions.