EBOOK

LORIKEET SECURITY

HIPAA, HITRUST, and SOC:

Common Compliance Frameworks Explained

HIPAA

Health Insurance Portability and Accountability Act

Mandatory for organizations handling health data. Covers PHI privacy, security, and breach notification. Penetration testing validates technical safeguards.

HITRUST

Health Information Trust Alliance

Certifiable framework (e1/i1/r2) integrating HIPAA, NIST, ISO 27001, and more. The enterprise gold standard for proving security posture.

SOC 2

Service Organization Controls Type 2

The SaaS and technology industry standard. Five Trust Services Criteria covering security, availability, confidentiality, integrity, and privacy.

INTRODUCTION

What You'll Learn In This Guide

Regulators and enterprise customers expect proof that you take security seriously. Whether you process health records, store financial data, or provide SaaS services, compliance is not optional. This guide breaks down HIPAA, HITRUST, and SOC, the three frameworks most commonly required by healthcare organizations, enterprise buyers, and security auditors, and explains exactly how penetration testing maps to each one.

SECTION 1

HIPAA

Purpose and scope, PHI definitions, Privacy vs Security Rule, compliance requirements, and where penetration testing fits.

SECTION 2

HITRUST

CSF overview, e1/i1/r2 assessment types, the certification path, and how pentest evidence satisfies assessor requirements.

SECTION 3

SOC

SOC 1/2/3 breakdown, Type 1 vs Type 2 differences, Trust Services Criteria, and SOC 2 audit preparation steps.

SECTION 4

Comparative Analysis

Side-by-side framework comparison and how Lorikeet Security supports all three in a single engagement.

Lorikeet Security covers all three frameworks

One pentest engagement. Evidence mapped to HIPAA, HITRUST, and SOC 2.
Audit-ready reports accepted by our CPA and HITRUST assessor partners.

CONTENTS

Table of Contents

SECTION 01

HIPAA (Health Insurance Portability and Accountability Act)

Purpose and Scope

HIPAA was enacted in 1996 to establish national standards for the protection of electronic health information. It created the Privacy Rule and Security Rule, which together govern how covered entities and business associates handle Protected Health Information (PHI). Any organization that creates, receives, maintains, or transmits PHI is subject to HIPAA, including healthcare providers, health plans, clearinghouses, and their vendors.

> ***"HIPAA violations most often stem from internal oversights rather than external attacks. A well-scoped penetration test closes that gap before regulators find it."***

Privacy Rule vs. Security Rule

Privacy Rule

All forms of PHI

Sets standards for when PHI may be used or disclosed. Patients retain rights to access and correct their records.

Security Rule

Electronic PHI (ePHI) only

Mandates administrative, physical, and technical safeguards. The rule that penetration testing most directly validates.

What Qualifies as Protected Health Information (PHI)?

- Names, dates, geographic identifiers, phone and fax numbers
- Social Security Numbers, account and certificate numbers
- Medical record and health plan beneficiary numbers
- Biometric identifiers: fingerprints, voice prints, retinal scans
- Full-face photographs and comparable identifying images
- Device identifiers, serial numbers, URLs, and IP addresses
- Health plan beneficiary numbers and certificate or license numbers
- Vehicle identifiers and serial numbers including license plates

Why PHI Protection Requires Penetration Testing

HIPAA violations most often stem from technical gaps, not deliberate breaches.
A penetration test finds those gaps before attackers, or regulators, do.

HIPAA Compliance Requirements

HIPAA compliance is a mandatory, continuous process. There is no official certification, but organizations must demonstrate adherence through documented policies, risk assessments, employee training, and technical controls. Enterprise customers and auditors increasingly require evidence of penetration testing to verify security posture.

Key Steps to Maintain HIPAA Compliance

01 **Establish policies and procedures**
Cover Privacy, Security, and Breach Notification Rules. Tailor to your organization and review annually.

02 **Appoint a HIPAA Officer**
A designated Privacy and Security Officer owns policy development, management, and enforcement.

03 **Train all employees**
Cover HIPAA obligations on hire and annually thereafter. Awareness reduces the insider risk behind most violations.

04 **Implement technical safeguards**
Encryption, secure storage, access controls, and proper disposal of ePHI at rest and in transit.

05 **Conduct regular risk assessments**
Identify and mitigate vulnerabilities to PHI confidentiality, integrity, and availability.

06 **Manage Business Associate Agreements**
Every vendor that touches PHI must sign a BAA. No exceptions, no informal arrangements.

07 **Build an incident response plan**
Document and test breach notification procedures. Know exactly what to do when something goes wrong.

08 **Perform penetration testing**
Validates that technical safeguards work against real-world attack techniques. Expected by auditors.

HIPAA by the Numbers

$10.9M	$100K-$50K	60%	500+
Largest HIPAA fine ever issued	Per-violation penalty range	negligence Of breaches stem from insider	annually Breaches reported to HHS

Most Common HIPAA Violations

- No encryption on devices or media containing ePHI
- Unauthorized employee access to patient records
- Missing or unsigned Business Associate Agreements
- Failure to conduct a formal or documented risk analysis
- Inadequate access controls and audit logging on ePHI systems
- Improper disposal of PHI on paper records or decommissioned hardware
- Outdated or absent workforce security awareness training

How Lorikeet Security Supports HIPAA

We perform HIPAA-scoped penetration tests that validate ePHI technical safeguards and generate risk analysis documentation accepted by HIPAA auditors.

Free retesting included. Proposal within 24 hours.

SECTION 02

HITRUST (Health Information Trust Alliance)

Background and Importance

HITRUST developed the HITRUST CSF (Common Security Framework), a certifiable framework that integrates requirements from HIPAA, NIST, ISO 27001, GDPR, and other regulations into a single adaptable standard. Originally healthcare-focused, HITRUST now serves any industry handling sensitive or regulated data. It is the gold standard for organizations that need to demonstrate their security posture to enterprise customers and regulators.

> ***"The HITRUST Framework is threat-adaptive, continuously updated to reflect emerging cyber threats, evolving regulations, and new compliance mandates."***

The Three HITRUST Assessment Types

e1

44 Controls 1-Year Certification

For low-risk organizations. Establishes baseline cybersecurity hygiene. Fastest path to a HITRUST credential.

i1

182 Controls 1-Year Certification

Moderate risk. Covers cybersecurity leading practices across a broader threat landscape than e1.

r2

250 to 1800 Controls 2-Year Certification

High assurance. Comprehensive risk-based controls. Required by most enterprise and government customers. Includes NIST CSF certification.

Structure and Implementation

HITRUST certification follows a structured five-stage path. Only HITRUST-approved assessor firms can perform the validated assessment required for certification. Working with an approved assessor from the outset avoids wasted effort and ensures evidence meets QA requirements.

The Five-Stage Certification Path

01 Readiness Assessment
Evaluate current posture against HITRUST requirements. Strongly recommended before any formal assessment to avoid costly surprises.

02 Self-Assessment
Use the MyCSF tool to identify control gaps ahead of the validated assessment. Available for all assessment types.

03 Validated Assessment
A HITRUST-approved external assessor formally evaluates your compliance with the CSF. This step is required for certification.

04 Remediation
Address all gaps and weaknesses identified in the validated assessment before submitting results to HITRUST.

05 Validation and Certification
Results are submitted to HITRUST QA for review. Certification is issued based on scores achieved.

Assessment Types at a Glance

	e1 Validated	i1 Validated	r2 Validated
Total Controls	44 (Fixed)	182 (Fixed)	250 to 1800
Certification Period	1 Year	1 Year	2 Years
Privacy Controls Included	No	No	Yes
NIST CSF Certification	No	No	Yes
Pentest Evidence Expected	Recommended	Expected	Required

What's New in HITRUST CSF v11.3

FedRAMP, StateRAMP, and TX-RAMP integration

Standardized approach for assessed entities doing business with government agencies.

NIST SP 800-172 integration

Enhanced protections for Controlled Unclassified Information (CUI) in r2 assessments.

CMMC Level 3 foundation

Prepares organizations for stringent NIST-based defense contractor compliance requirements.

MITRE Atlas AI mitigations

Addresses security controls specifically for the protection of AI systems and agents.

Streamlined assessment process

Reduced redundancy in requirement statements, meaningfully decreasing r2 assessment size.

Penetration Testing and HITRUST

HITRUST CSF control categories covering communications, operations management, and access control directly reference penetration testing and vulnerability assessments as validation methods. For r2 assessments, assessors expect documented evidence of penetration test results mapped to the relevant HITRUST control domains. A report that does not map to HITRUST categories will not satisfy assessor evidence requirements.

SECTION 03

SOC (Service Organization Controls)

Overview of the SOC Framework

The SOC framework was developed by the American Institute of CPAs (AICPA) to help service organizations demonstrate the effectiveness of their internal controls. SOC reports give customers and auditors transparency into how a service provider manages the risks that affect their clients' data and systems. SOC 2 has become the de facto security standard for technology and SaaS companies worldwide.

The Three SOC Report Types

SOC 1

Internal controls over financial reporting (ICFR). Relevant for service providers whose operations directly affect customer financial statements.

SOC 2

Controls over security, availability, processing integrity, confidentiality, and privacy. The standard for technology companies. Penetration testing is expected by auditors.

SOC 3

A simplified, public-facing summary of a SOC 2 report. Can be published as a trust seal on a website. Requires a completed SOC 2 audit first.

SOC 2: Type 1 vs. Type 2

Type 1

Point-in-time design assessment

Evaluates whether controls are suitably designed at a single moment in time. Faster to achieve. Good for initial customer trust and early-stage compliance.

Type 2

Operational effectiveness over time

Evaluates controls over a defined 6-12 month observation period. Higher assurance. Required by most enterprise buyers, investors, and regulated industries.

The Five Trust Services Criteria

Security CC6

The system is protected against unauthorized access. This is the only mandatory criterion and the one penetration testing most directly validates.

Availability A1

The system is available for operation as committed. Covers uptime SLAs, DDoS mitigation, and disaster recovery capabilities.

Processing Integrity PI1

System processing is complete, valid, accurate, timely, and authorized. Relevant for financial and transaction processing services.

Confidentiality C1

Information designated as confidential is protected as committed or agreed in service agreements and privacy notices.

Privacy P1-P8

Personal information is collected, used, retained, disclosed, and disposed of according to the published privacy notice.

Penetration Testing and SOC 2

SOC 2 CC6 explicitly expects evidence that organizations test their technical controls. Auditors look for penetration test results as evidence that CC6.1 (access restrictions), CC6.6 (boundary protection), and CC7.2 (vulnerability management) controls are operating effectively. Most SOC 2 Type 2 auditors will flag a missing penetration test as a gap in the control environment.

Lorikeet Security + Accorp Partners CPA

We handle the penetration testing. Accorp delivers the SOC 2 Type 1 or Type 2 attestation. One intake call. Auditor-ready findings on the first pass.

Free retesting included. Proposal within 24 hours.

Steps to Prepare for a SOC 2 Audit

Most companies underestimate the preparation a SOC 2 audit requires. Starting 6 to 9 months before your target attestation date gives enough runway for the observation period, control development, gap remediation, and retesting.

01 **Identify applicable Trust Services Criteria**
Security (CC6) is mandatory. Determine which of the other four criteria apply to your services and customer commitments.

02 **Define the scope**
Identify which systems, infrastructure, applications, and personnel fall within the audit boundary.

03 **Conduct a risk assessment**
Map your control environment against the Trust Services Criteria and identify gaps that need remediation.

04 **Develop or update controls**
Build or improve policies and technical controls to address every identified gap.

05 **Implement employee security training**
Security awareness training is itself a control requirement, not optional background activity.

06 **Document all policies and procedures**
Auditors require written evidence that controls exist, are communicated, and are enforced consistently.

07 **Select a qualified CPA auditor**
Must be a licensed CPA firm. Lorikeet partners with Accorp Partners CPA for SOC 2 attestation.

08 **Perform penetration testing**
Validates CC6 and CC7 technical controls. Expected evidence by most SOC 2 Type 2 auditors.

09 **Remediate findings before audit window closes**
Fix issues from the pentest and gap analysis before the observation period ends.

SECTION 04

Comparative Analysis and How Lorikeet Helps

Framework Comparison at a Glance

	HIPAA	HITRUST	SOC 2
Certification available	No	Yes (e1 / i1 / r2)	Yes (Type 1 / 2)
Primary audience	Healthcare orgs	Any regulated data	Technology / SaaS
Pentest requirement	Strongly implied	Required for r2	Expected for CC6
Credential validity	Ongoing	1 to 2 years	Annual
Auditor required	No formal audit	HITRUST-approved firm	Licensed CPA firm
Privacy controls	Yes	Yes (r2 only)	Optional (P1-P8)
Overlaps with	SOC 2	HIPAA, NIST, GDPR	HIPAA, HITRUST

Most organizations do not need to choose just one framework. A healthcare SaaS company will often need HIPAA compliance, HITRUST certification to satisfy enterprise customers, and SOC 2 for general market trust. A single, well-scoped penetration test from Lorikeet Security generates mapped evidence for all three, reducing cost and coordination overhead significantly.

> ***"Compliance is not just a regulatory requirement. For businesses handling sensitive data, it is a strategic asset that reinforces integrity and builds customer trust."***

How Lorikeet Security Supports All Three

Every compliance framework in this guide expects evidence that your security controls actually work. Lorikeet Security provides the penetration testing that generates that evidence, with reports formatted for each framework's specific documentation requirements.

HIPAA Penetration Testing

`lorikeetsecurity.com/service-areas/hipaa-pentest`

Technical validation of ePHI safeguards. Reports formatted for HIPAA risk analysis documentation and accepted by HIPAA auditors on the first pass.

HITRUST Penetration Testing

`lorikeetsecurity.com/service-areas/hitrust-pentest`

Findings mapped directly to HITRUST CSF control categories. Supports e1, i1, and r2 validated assessments without additional mapping work.

SOC 2 Penetration Testing

`lorikeetsecurity.com/service-areas/soc2-pentest`

Trust Service Criteria-mapped reports. Paired with Accorp Partners CPA for full SOC 2 Type 1 and Type 2 attestation in one coordinated engagement.

Compliance Bundle

`lorikeetsecurity.com/packages`

One engagement. Evidence mapped to HIPAA, HITRUST, and SOC 2 simultaneously. Reduces cost and eliminates coordination overhead across all three frameworks.

What Makes Lorikeet Different

- 100% manual testing. No automated scanner output passed off as penetration testing.
- Free retesting included on every engagement. We verify every fix at no extra charge.
- Audit-ready reports on the first pass. Accepted by our CPA and HITRUST assessor partners.
- Proposal within 24 hours. Testing starts within 1 to 2 weeks of engagement kickoff.
- Direct access to your testing team throughout the engagement. No account managers.

LORIKEET SECURITY

Ready to get compliant?

Human First, AI-Powered Security. Proposal in 24 hours.

HIPAA Penetration Testing

Technical validation of ePHI safeguards. Reports formatted for auditor review.

lorikeetsecurity.com/service-areas/hipaa-pentest

HITRUST Penetration Testing

Findings mapped to HITRUST CSF categories for e1, i1, and r2 assessments.

lorikeetsecurity.com/service-areas/hitrust-pentest

SOC 2 Penetration Testing

Trust Service Criteria-mapped reports. Paired with Accorp Partners CPA.

lorikeetsecurity.com/service-areas/soc2-pentest

Compliance Bundle

One engagement. Evidence for HIPAA, HITRUST, and SOC 2 simultaneously.

lorikeetsecurity.com/packages

Book a Free Consultation

lorikeetsecurity.com/contact | (888) 652-6479

(888) 652-6479
Toll-Free

sales@lorikeetsecurity.com
24-hour response

(929) 577-3213
New York, NY

About Lorikeet Security

Lorikeet Security (Lorikeet Corp) is a human-first, AI-powered penetration testing and security consulting firm serving startups, SaaS companies, healthcare organizations, and enterprises. We combine certified offensive security expertise with Lory, our AI security assistant, to deliver thorough, audit-ready assessments across all major compliance frameworks.