

CyberSec Frameworks

SaaS Companies, Payment Processors, MSPs & Security Teams

"SOC 2. ISO 27001. PCI-DSS. One team. One platform. No overlap."

Technology companies face a patchwork of security frameworks demanded by customers, partners, and regulators — often simultaneously. Auditerra's multi-framework approach eliminates duplication, maps overlapping controls across SOC 2, ISO 27001, PCI-DSS, and NIST CSF, and delivers audit readiness continuously — not just when a prospect asks for your SOC 2 report.

SOC 2 Type II

ISO 27001:2022

PCI-DSS v4.0

NIST CSF 2.0

The Challenge

- Sales cycles increasingly stall on security questionnaires and missing SOC 2 reports — compliance is now a revenue issue, not just a risk issue.
- Managing multiple frameworks independently creates redundant evidence collection, inconsistent documentation, and audit fatigue across engineering and security teams.
- ISO 27001:2022 introduced 11 new controls that many organizations have not yet mapped to existing SOC 2 or NIST programs.
- PCI-DSS v4.0 shifts responsibility to organizations to define their own targeted risk analysis approaches — a material change from prior versions.
- MSPs and MSSPs face customer-imposed audit obligations across dozens of client environments with varying framework requirements.

Compliance Frameworks We Cover

SOC 2 Type II

The de facto standard for SaaS companies. Covers Security, Availability, Confidentiality, Processing Integrity, and Privacy trust service criteria. Type II requires evidence over a defined observation period.

ISO 27001:2022

International standard for Information Security Management Systems (ISMS). The 2022 revision added 11 new controls across threat intelligence, cloud security, and data masking. Certification is performed by accredited external auditors.

PCI-DSS v4.0

Applies to any organization that stores, processes, or transmits cardholder data. v4.0 introduces customized implementation options and new requirements for targeted risk analysis and authentication controls.

NIST CSF 2.0

The updated framework adds a new Govern function and expanded guidance for supply chain risk management. Increasingly used as an enterprise security governance baseline alongside certifiable frameworks.

SOC 2 + ISO 27001 Dual Certification

Auditerra's multi-framework approach maps overlapping controls so evidence collected for one framework satisfies requirements in others — reducing audit burden by up to 40%.

How Auditerra Engages — Our Process

Step 1 — Demo

A no-pressure, industry-tailored demo so you see exactly how our platform and auditors work together before any commitment.

Step 2 — Readiness Check

We conduct a gap assessment to map your current compliance posture, identify risk areas, and build a prioritized remediation roadmap.

Step 3 — Active Engagement

Our certified auditors don't hand you a to-do list. They work alongside your team — reviewing evidence, walking through controls, and personally resolving gaps in real time.

Step 4 — Continuous Monitoring

Compliance doesn't end at certification. Auditerra monitors your posture year-round, alerts you to drift, and keeps you audit-ready at all times — not just during audit season.

Why Not Big 5 or SaaS-Only?

Provider	What You Get	What's Missing
Big 5 Consulting	Deep expertise, global reach	Enterprise pricing — out of reach for most
SaaS-Only Platforms	Evidence collection platform	No human auditor — you're on your own
Auditerra	Platform + certified human auditors	Nothing. Custom pricing. Full engagement.

Multi-Framework Strategy — Eliminate the Duplication Tax

The most costly mistake technology companies make is treating each compliance framework as a separate project. SOC 2 and ISO 27001 share a significant control overlap — when mapped correctly, a single evidence artifact can satisfy requirements in both. Auditerra's platform maintains a unified control library that maps your policies, configurations, and evidence to every applicable framework simultaneously. When a new framework is added — say, PCI-DSS after a new payment product — we identify what you already have, what's missing, and build only what's new. The result: faster time-to-certification, less burden on your engineering team, and a compliance posture that actually scales with your product.

What You Get with Auditerra

- ✓ Unified control mapping across SOC 2, ISO 27001:2022, PCI-DSS v4.0, and NIST CSF
 - ✓ SOC 2 Type II audit preparation and evidence management with auditor coordination
 - ✓ ISO 27001:2022 gap assessment against all 93 Annex A controls including new additions
 - ✓ PCI-DSS v4.0 Targeted Risk Analysis development and Requirement 12 compliance program
 - ✓ Continuous monitoring with automated control testing and drift alerting
 - ✓ Security questionnaire library for faster enterprise sales responses
-

Ready to See It in Action?

Book your no-obligation demo at auditer.com/demo or reach out directly at compliance@auditer.com. We'll tailor the conversation to your industry, your frameworks, and your timeline — no generic pitch decks.