INDUSTRY USE CASE

Legal & Professional Services

Law Firms, Accounting Firms & Consulting Practices

"Client confidentiality is non-negotiable. So is your compliance program."

Law firms, accounting practices, and consulting firms are high-value targets for cybercriminals precisely because of the sensitive client data they hold — M&A; plans, litigation strategy, financial records, personal information. Enterprise clients now routinely require SOC 2 reports, ISO 27001 certification, and GDPR/CCPA compliance documentation before engaging professional services firms. Auditerra helps professional services firms build programs that satisfy client due diligence and protect the confidentiality obligations at the heart of their practice.

SOC 2 Type II | ISO 27001 | GDPR | CCPA/CPRA | ABA Guidelines

The Challenge

- Enterprise and financial services clients increasingly require SOC 2 Type II reports or ISO 27001 certification as a prerequisite for engagement — and deals stall when firms can't produce them.
- Law firms hold attorney-client privileged communications, litigation files, and M&A; deal information that represent extraordinarily high-value targets for nation-state and criminal threat actors.
- GDPR and CCPA obligations apply to professional services firms handling personal data of EU or California residents — a common scenario for any firm with international clients or matters.
- Accounting firms subject to PCAOB oversight face additional scrutiny of their own cybersecurity programs as regulators assess whether audit quality is compromised by inadequate firm security.
- Remote work and cloud-based practice management platforms have expanded the attack surface dramatically — often without corresponding security program updates.

Compliance Frameworks We Cover

SOC 2 Type II

The primary assurance mechanism demanded by enterprise clients in legal, financial, and technology sectors. Demonstrates that the firm's security, confidentiality, and availability controls meet recognized standards.

ISO 27001:2022

International certification increasingly required by global enterprise clients and multinational matters. Provides a structured ISMS that maps to client security requirements across jurisdictions.

GDPR

Applies to any firm handling personal data of EU residents. Requires documented lawful basis for processing, data subject rights procedures, breach notification within 72 hours, and DPA agreements with processors.

CCPA / CPRA

California's privacy framework applies to firms meeting threshold criteria for California resident data. Requires privacy notices, opt-out mechanisms, and documented data inventory.

ABA Cybersecurity Guidelines

The American Bar Association's ethics opinions and cybersecurity guidelines establish professional responsibility obligations for law firms to protect client data and competently manage cyber risk.

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.

Client Due Diligence & Confidentiality Obligation Compliance

Professional services firms operate under a fundamental confidentiality obligation that makes cybersecurity compliance a professional responsibility issue — not just a business risk issue. A breach of client data is a breach of trust that can trigger bar complaints, malpractice exposure, and client defection simultaneously. Auditerra builds compliance programs that start with the firm's most sensitive data — client matter files, financial records, privileged communications — and work outward to the systems and vendors that touch them. We help firms respond to enterprise client security questionnaires, produce SOC 2 reports that accelerate business development, and build GDPR-compliant data processing frameworks for international practice areas. Our auditors understand the professional services environment: partnership structures, matter-based data organization, and the practical constraints of implementing security in a billable-hour culture.

What You Get with Auditerra

- ✓ SOC 2 Type II readiness assessment and audit preparation for client due diligence requirements
- ✓ ISO 27001:2022 gap assessment and certification roadmap for international client requirements
- ✓ GDPR compliance program including data inventory, lawful basis documentation, and DPA agreements
- ✓ CCPA/CPRA privacy program and data subject rights workflow implementation
- ✓ Security questionnaire library and response program for enterprise RFP/due diligence processes
- ✓ Continuous monitoring with matter-aware data classification and access control verification

---

Ready to See It in Action?

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