PRESCIENT SECURITY

ISO 27001 with Prescient Security

What is ISO 27001

At Prescient Security we approach each ISO 27001 engagement as security practitioners, which means we test how ISMS operates, trace risk through your controls, and produce findings for engineering and GRC teams. Additionally we keep clean lines with vCISO partners and GRC platforms supporting readiness, while we deliver independent certification. Clients receive observations mapped to ISO 27001 and Annex A controls, risk-based severity, cross-framework references (e.g., SOC 2, HIPAA, PCI) as well as practical remediation guidance. This combination gives operators a playbook for fixes and stakeholders the needed evidence. We strictly follow the official ISO 17021-1, ISO 27002, and ISO 27006 standards to ensure a high quality professional audit.

What problem we solve

Most teams are stuck between traditional registrars who treat ISO as paperwork and consultancy bundles that can blur independence. Documentation-only audits miss operational and security risks and drag out timelines all while generating reports that don't translate into real risk mitigation. Bundles that include "readiness + certification" introduces conflicts of interest and undermines credibility with customers and regulators.

Prescient Security closes this gap for organizations that sell into enterprises and operate under due-diligence and regulatory scrutiny. You get an independent certification motion that ties directly to risks and aligns with your other frameworks. Also important, it produces reusable evidence for customer reviews, cyber-insurance, and internal reporting. All this without compromising the integrity of the audit. We are also the first offensive security company to offer ISO certifications.

How it works

We start with context. Auditors map your business objectives, risk assessment, asset inventory, and control environment. We trace key flows across a few main main points: identity and access, change and deployment, vendor risk, incident response, backup and recovery, monitoring, and secure development. This ensures that risk-first view focuses on audit depth where impact is highest.

Additional we run an organized certification process:

1. **Stage 1 Readiness for certification:** Review ISMS scope, policies, risk methodology, Statement of Applicability, and evidence for design maturity. Identify gaps tied to ISO 27001.
2. **Stage 2 Certification:** Test operating effectiveness across selected samples, interviews, technical demonstrations, and control walk-throughs. Integrate security context like vulnerability and penetration test results.
3. **Ongoing assurance**: Annual surveillance audits maintain certification; triennial recertification resets the cycle with a fresh risk-driven scope.

Before anything reaches you, findings go through internal QA. Each issue includes control mapping, risk impact, examples of acceptable evidence, and cross-framework references. It allows the client to update policies or tickets which can be reused across audits and customer due diligence.

We preserve independence by partnering with vCISO firms and integrating smoothly with GRC platforms for evidence exchange and status tracking.

Key benefits

Security-first certification
Audits that focus on operational risk and control effectiveness

Multi-framework Audit Services
Evidence and mappings reusable for ISO 27701, 22301,42001, 20000-1,27017,27018, SOC 2, HIPAA, PCI DSS, FedRAMP, CMMC, c4/c5, etc.

Actionable outputs
Clause-mapped findings with risk context, and stepwise remediation that engineering and GRC teams can execute

Predictable cadence
Stage 1/Stage 2 certification followed by annual surveillance and three-year recertification

Independent credibility
COI boundaries between readiness and certification

Built for teams managing more than one framework

Most of our clients need additional frameworks besides ISO 27001. We align audit scope and evidence across SOC 2, HIPAA, HITRUST, PCI DSS, and NIST so you're not duplicating work or juggling multiple firms. Talk to a Prescient Security expert to plan your ISO 27001 engagement.