



ANCORA
CYBER

CASE STUDY

Accelerating Dual ISO 27001 &
SOC 2 Success for a High-
Growth SaaS Provider

CASE STUDY

Accelerating Dual ISO 27001 & SOC 2 Success for a High-Growth SaaS Provider



Overview

A rapidly scaling SaaS organization operating in a highly regulated market approached Ancora Cyber with an urgent challenge: achieve ISO 27001 certification and SOC 2 attestation, both within a 9-month window, in order to satisfy contractual requirements and secure a landmark enterprise deal.

Despite the tight timeline, the client successfully passed both audits with zero exceptions and zero nonconformities, earning a clean ISO 27001 certification and a flawless SOC 2 report. These results positioned them to close their largest customer to date and strengthened their overall security posture.

Challenges

The client contacted Ancora Cyber with a clear mandate and an aggressive deadline:

“We need to be fully audit-ready for ISO 27001 and SOC 2, both, within 9 months.”

As an organization with evolving processes, limited documentation, and a fast-moving engineering culture, they needed a partner who could:

- ✓ Build a security program aligned to global standards
- ✓ Identify and mitigate real risks
- ✓ Prepare leadership and staff for external audit scrutiny
- ✓ Do it all without slowing down product innovation

Ancora Cyber’s team immediately mobilized.

Solutions

Technical & Governance Foundations

We began with our Governance, Risk, and Compliance (GRC) team performing a comprehensive company-wide Risk Assessment, cataloging the organization's most pressing risks and identifying gaps that could affect audit readiness.

Security Architecture & Threat Modeling

Next, Ancora Cyber facilitated an intensive Security Architecture Workshop with engineering and product leadership. We examined:

- Network and infrastructure design
- Data handling and flow patterns
- Access controls and identity management
- Operational processes and inherited risks

Following this workshop, our threat analysts conducted an in-depth Threat Assessment, modeling realistic attack scenarios based on the client's industry profile and technology stack. We then delivered a prioritized roadmap to mitigate risks and strengthen controls.

Program Development & Documentation

To operationalize the client's security program, we:

- Evaluated and enhanced their Security Awareness program
- Authored core ISO 27001-required documentation
- Performed the heavy lifting to operationalize the program
- Formalized ongoing security activities and governance practices
- Built repeatable, auditable processes aligned with ISO 27001 and SOC 2
- Delivered Management Review guidance and facilitation
- Provided Pre-Audit Training for executives and control owners

Pre-Audit Internal Review

Our consultants executed a rigorous pre-audit assessment, mirroring the structure and scrutiny of an external audit. This helped validate control maturity, uncover remaining gaps, and ensure leadership and staff were confident before engaging the certification body and CPA firm.

Our Approach

Ancora Cyber applies a proven security program development methodology that blends the structure of ISO 27001's Information Security Management System (ISMS) with the practicality of NIST's Risk Management Framework (RMF).

This approach allows clients to mature quickly, reduce waste, and improve audit outcomes without disruption.

Risk Assessment

Working closely with leadership and technical teams, we:

- Defined the scope of the security program
- Identified critical assets, threats, and vulnerabilities
- Assessed likelihood and potential business impact
- Prioritized risk treatment based on real-world conditions

The result: A clear, actionable understanding of what mattered most.

Implementation

Ancora Cyber collaborated directly with client stakeholders to:

- Build and document their security policies
- Improve vulnerability management workflows
- Establish ongoing compliance cadence
- Implement processes necessary for continuous improvement

By this stage, the client had a fully functional and maturing security program capable of meeting and sustaining ISO and SOC requirements.

Pre-Audit Assistance

With the program in place, we guided them through:

- An internal audit to simulate external testing
- Corrective actions and residual risk handling
- A formal Management Review meeting
- Preparation of control owners and leadership for interviews
- Requests-list readiness, evidence preparation, and logistics

This removed uncertainty and ensured complete readiness for the external audit teams.

Results

The client achieved audit readiness ahead of schedule, ultimately:

- ✓ Passing both ISO 27001 certification and SOC 2 attestation on the first attempt
- ✓ Receiving zero findings from external auditors
- ✓ Avoiding costly tooling investments, technical debt, or last-minute rework
- ✓ Strengthening customer confidence and brand credibility
- ✓ Accelerating revenue by unlocking enterprise-level deals

Ancora Cyber delivered a seamless experience and earned a long-term partner in the process.

Fast-Forward

Today, the client continues to maintain both ISO 27001 and SOC 2 compliance through Ancora Cyber's Continuous Management Services. Our team operates as an extension of their organization, overseeing:

- Policy and procedure updates
- Annual risk and internal audit cycles
- Continuous improvement activities
- Ongoing audit support
- Evidence collection and control operation guidance

As a result, they continue to pass their annual audits with confidence, year after year.

**Start With a Mapping
Conversation |**

850.240.3384
chris@ancoracyber.com