

Compliance & Audit Readiness

Golden Volunteer: vCISO & Continuous SOC 2 Compliance

How Nexeris took over Golden's security program operations, keeping SOC 2 Type 2 compliance running year-round without pulling engineering teams off product work.

CLIENT

Golden Volunteer

ENGAGEMENT TYPE

vCISO & Continuous SOC 2
Compliance Management

INDUSTRY

Volunteer Management Software / Technology



Overview & The Challenge

Continuous SOC 2 Type 2 compliance delivered for a lean software team without disrupting product development.

CLIENT PROFILE

CLIENT

Golden Volunteer

INDUSTRY

Volunteer Management Software, Technology

COMPLIANCE LEVEL

SOC 2 Type 2, HIPAA

KEY ACHIEVEMENT



90%+

Compliance Workload Reduction

Zero Exceptions or Major Findings Across Annual Audit Cycles

Offloaded over 90% of compliance and security program management from Golden's internal engineering and operations teams while maintaining continuous SOC 2 Type 2 audit readiness.

THE CHALLENGE

After successfully achieving their initial SOC 2 Type 1 and Type 2 compliance, Golden faced the ongoing challenge of maintaining compliance year-round for their annual SOC 2 Type 2 audits. To manage this, Golden utilized Vanta as their GRC platform. However, the platform required continuous monitoring, prompt remediation of failing automated tests, constant evidence gathering, and regular security program operations including risk assessments, vendor reviews, and access audits.

Without dedicated security staff, managing Vanta and the broader security program was overwhelming Golden's core development and operations teams, distracting them from product growth while exposing them to the risk of compliance gaps during their Type 2 audit window.

WHAT WAS AT RISK

- ▶ Annual SOC 2 Type 2 audit success at risk without continuous year-round compliance operations.
- ▶ Core engineering and operations teams overwhelmed by GRC management burden.
- ▶ Compliance gaps and audit exceptions threatening key enterprise contracts and client trust.

The Solution

Nexeris took over Golden's full security program operations, managing Vanta and running continuous compliance so the internal team never had to.



VCISO AND COMPLIANCE-AS-A-SERVICE (CAAS)

Nexeris delivered an ongoing program of security expertise, serving as Golden's on-demand security resource to mature and operate their security program.



ACTIVE VANTA MANAGEMENT

We took over continuous management of Golden's Vanta instance. This included configuring integrations, validating automated tests for accuracy against actual production environments, investigating and remediating system alerts, and ensuring all continuous evidence is automatically and accurately collected without manual intervention.



CONTINUOUS COMPLIANCE OPERATIONS

Nexeris managed and executed Golden's year-round compliance requirements, including conducting annual risk assessments, performing vendor security reviews, facilitating quarterly access reviews, and running business continuity (BC/DR) and incident response tabletop exercises.



AUDIT REPRESENTATION

Serving as Golden's primary security representatives, we directly represented Golden during their annual SOC 2 Type 2 audits, handling auditor requests, compiling supplemental manual screenshots or artifacts when automated tests lacked audit-level depth, and addressing any technical inquiries from the audit team.

THE RESULTS



90%+

Compliance Workload
Reduction / Offloaded from
Internal Teams

SOC 2 TYPE 2 COMPLIANCE MAINTAINED YEAR-ROUND

Golden passed their annual SOC 2 Type 2 audits with zero major exceptions or findings, preserving client trust and protecting key enterprise contracts. With Nexeris managing the full compliance program, Golden's engineering and operations teams were freed to focus entirely on product growth.

- ✓ Zero exceptions or major findings across annual SOC 2 Type 2 audit cycles
- ✓ Over 90% of compliance workload removed from internal engineering and operations teams
- ✓ Vanta instance kept continuously green, verified, and audit-ready at all times
- ✓ Full year-round security program operations managed without internal resource drain

“

"Nexeris helped us gain clarity for our security program's growth needs and also took the time to properly understand our needs to ensure our ongoing success."

Michael Collier

Engineering Program Director,
Golden Volunteer



Golden



Key Takeaways



GRC PLATFORMS NEED HUMAN EXPERTS

Automated compliance platforms like Vanta are incredibly powerful for tracking, but they do not run themselves. Human expertise is required to configure tests correctly, interpret failing alerts, and handle the organizational controls (like tabletop exercises and vendor assessments) that cannot be automated.



SOC 2 TYPE 2 REQUIRES CONTINUOUS EFFORT

Unlike Type 1, which represents a single point in time, Type 2 compliance requires demonstrating operating effectiveness over a 12-month period. Partnering with a vCISO service ensures that security controls are consistently executed throughout the year, eliminating the panic of audit prep and preventing costly audit exceptions.