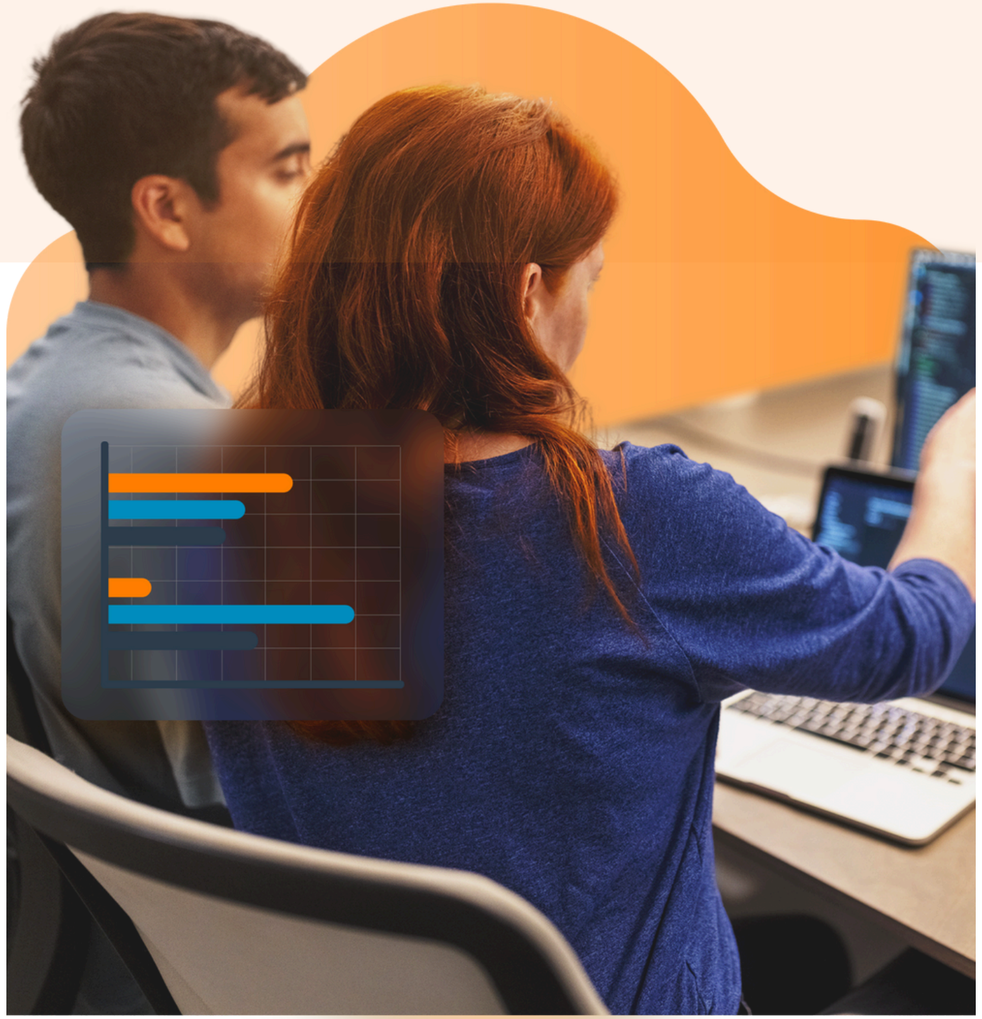
asureti

Managed Assurance - Building a GRC Program

Case Study

Enterprise Application SaaS Platform

Colorado, United States



Founded in 2016, this company delivers software and applications required for businesses to thrive in the digital era.

Key figures:

- Serving over 1,000 clients around the world.
- Over 450 employees.

asureti

The Challenge

This company contacted Asureti needing a SOC2 to meet current customer requirements. The lack of having a SOC2 in place put their current and future revenue goals at risk! With no formal GRC program, and without an internal compliance team, their executive and board leadership lacked the knowledge and experience of GRC compliance, and the insight needed to manage their risk and audit defense.

Challenges from New Client Requirements

Gaps in Required Processes & Documentation

Missing documentation and internal processes required for a SOC2 attestation.

Experience Gap

No internal resources with experience in building and operating necessary risk assessment and GRC program operations.

Limited Bandwidth & Budget

With internal teams already allocated, needed a trusted partner to help build and maintain the required components.

asureti

Our Approach

We performed a systematic risk assessment that evaluated their current compliance state and ability to meet the necessary technical and process requirements to attain a SOC2. This process unlocked potential opportunities for their business and overcame existing hurdles caused by limited resource availability.

1. **Implemented a proven GRC platform** to aggregate key program information and streamline required operational activities.

2. **Reviewed multiple control sets** to assist in creating a new baseline across two brands being integrated post acquisition. This baseline would develop a continuity between the brands and combine controls where possible to increase efficiencies.

3. **Loaded baseline controls and policies into GRC platform** to support ongoing operations, including reviews and approvals. This provided a centralized place for them to gain the insight into their compliance program and control status.

asureti

Our Analysis

182

Controls Identified

During our review of the organization, we identified **182 controls** across **two brands** that needed to be formalized.

Implementing a GRC program provided a viable roadmap to follow for future success and allowed for a more efficient allocation of resources.

Without a trusted partner to build and manage a GRC program, they would run the risk of inconsistent or missed control operation, impacting the ability to achieve and maintain their SOC2 attestation as required by their clients.

asureti

Recommended Actions

Immediate:

- Continue leveraging **Asureti's Managed Assurance** to expand their compliance framework.
- Annual testing of 182 controls in support of the SOC process along with the review and update of 20 policies.
- Continue to perform NIST based IT risk assessments of 328 items considered at risk.

Long Term:

- Enhance third-party risk monitoring to make audit reviews more efficient.
- Build an enterprise risk management program and cross-train internal team to continue to mature the GRC program.

asureti

Project Recap

80%

SOC Report Exception Reduction

Partnering with trusted GRC experts allowed the SOC audit process to run more smoothly, alleviated audit fatigue, and reduced year-over-year SOC report exceptions by **80%.**

An annual roadmap provided continuity, efficiency, and audit-ready evidence to support ongoing regulatory and organizational requirements of GRC.

The delegation of the organization's GRC program tasks allowed their Compliance Director to focus on newly acquired security responsibilities without needing additional staff.

asureti

Similar Challenge?

Book a discovery call

Email

info@asureti.com

asureti