FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

CASE STUDY

SOC 2

CERTIFICATION

READINESS ASSISTANCE

Business Challenges

- SOC 2 Audit required by clients
- Internal IT team unsure how to prepare
- Failure to pass audit by deadline would result in lost revenue

Foresite Solution

- SOC 2 Readiness Assessment
- vCISO for remediation and audit support
- Incident Response retainer

Results

- Client successfully passed the audit and obtained SOC 2 certification on first attempt
- No loss of revenue
- Incident Response resources in place proactively

BACKGROUND

A contractor that provides data analytics faced a new SOC 2 requirement for renewal of a contract they previously held with a state government. The Director of IT requested assistance preparing for the audit to make sure it resulted in successful certification prior to the renewal date. While the contractor often dealt in regulated data and had a mature cybersecurity program, they were unsure of the specific requirements and nuances of SOC 2, and felt that without outside expertise, there was a good chance they might miss things that would cause them to not meet certification within the required time-frame. Foresite's GRC consultant began by conferring with the firm's stakeholders to identify their objectives for this project.

OBJECTIVES

- ☐ Properly scope the SOC 2 principles that applied and systems
- ☐ Identify the gaps that would cause failure of the audit
- ☐ Assist with remediation of gaps working with internal and 3rd party IT
- ☐ Establish a relationship with a cybersecurity firm that provides resources for aspects of cybersecurity that are required but out of the reach of a smaller organizations internal resources (such as Incident Response)
- ☐ Support for the certification audit

OUR SOLUTIONS

We recommended a SOC 2 Readiness Assessment to compare the firm's current policies and controls with trust services principles found in the AICPA's common criteria. We identified the principles that applied to the state governments ask, as well as the systems involved, in addition we identified any other systems that could impact the principles at play in the state governments ask.

Our findings were not unusual. While they had much of the security best-practices framework in place, there were some specific nuances to SOC 2 that were missing. Some policies and processes were not in place. Also, we found much of the required evidence collection and ongoing validation required to achieve a SOC 2 Type II Certification were not in place. Foresite filled in the gaps using consulting hours.

Utilizing our work product for SOC 2 Readiness we did a mock audit. Based on the mock audit results we worked with the client to prepare everything that would be required when the CPA firm performed the formal certification audit. When it came time for the audit, Foresite worked as a team member helping fulfill the requests of the auditor until the auditor felt comfortable certifying the contractor as a SOC 2 compliant and write a SOC 2 Type II Report for them to share with the state government. This occurred well within the time-frame required and the client could renew the service with the state government.

WORLD **HEADQUARTERS**
7311 West 132nd Street, Suite 305
Overland Park, KS 66213
+1 (800) 940-4699

CT **OFFICE**
1 Hartfield Blvd, Suite 300
East Windsor, CT 06088
info@foresite.com

UK **OFFICE**
A8 Ively Road, Farnborough
Hampshire, GU14 0LX UK
+44 (800) 358-4915