Apgar & Associates

Healthcare Tech SME leverages Apgar & Associates' SOC2 Prep Expertise

A Case Study in Setting the Competitive Bar

Case Study: Healthcare Technology SME | SOC2 Prep

Apgar & Associates

"Apgar & Associates' knowledge was invaluable in helping to **bridge the gap** between the auditor's understanding and our internal processes.

Plus, we never felt hampered or bogged down in costly practices – they've been true partners."

– Client CEO

Favorite Benefit
Day-to-Day Confidence in InfoSec program.

How it began

Healthcare Technology SME **determines SOC2 to be best fit** for market proof of infosec excellence, partners with consulting firm Apgar & Associates, LLC to **prep for SOC 2** certification process.

A growing healthcare software and services company chose to pursue SOC2 in Security as their badge of proof to the market that they not only prioritize information security, but also have the right controls in place to assure that security. They decided SOC2 best fit their objectives of a well-accepted industry standard as well as a doable timeframe for achievement.

Operationalizing data privacy and information security doesn't happen overnight, which is why the healthcare technology company started with a comprehensive Security Risk Analysis (SRA) led by Apgar & Associates prior to diving into the SOC2 prep process. Then they moved to the certification readiness phase.

"SOC2 – like other industry standards – demands thoroughness, dotting the ***i's*** and crossing the ***t's*** at every stage of the journey. For example, we needed to carefully define SOC2 controls and having a trusted sounding board who understood how we operated was crucial to doing that well," asserted the CTO.

Apgar and Associates has applied their certification readiness services to help many organizations succeed in SOC2, HITRUST, and ISO certifications. Having worked with the healthcare technology SME through the intricacies of a comprehensive Security Risk Analysis, Julia explained, **"They consistently demonstrated their dedication to maintaining a high level of security excellence.** Chris (Apgar) and I knew they were poised to dive into SOC2 prep."

What did the healthcare technology SME need from the partnership?

Consultative expertise and guidance throughout the process. They relied on Apgar & Associates to help overhaul policy and procedures while concurrently formalizing infosec activities. They also wanted to assure that the SOC2 auditor was one that worked with companies of a similar size and structure.

Case Study: Healthcare Technology SME | SOC2 Prep

What came next

At every step of the actual "prep process" Julia and Chris were the company's thought partners and tactical guides. They worked closely with the company team to define SOC2 controls and understand the overall attestation process. The Apgar team helped ensure that the defined SOC2 controls were 1) comprehensive enough for auditor standards and 2) accurately represented the healthcare technology SME's infosec program and operations. Additionally, Apgar & Associates helped to:

- Map controls to Common Criteria
- Determine what would be appropriate evidence
- Review the infosec activities to assure they met control evidence
- Run mock walkthroughs

The outcome

While the healthcare technology company felt confident in their operationalized infosec activities, they also knew the positive impact that a successful SOC2 attestation would have on new service or product offerings. "Any new initiatives will – from the outset - 100% fit in with the controls we've put in place. In fact, we're already doing it with our latest product, with operational checks and balances as part of the infosec calendar," the COO shared.

The company has confidence that they'll continue active information security practices actively simply because those live at the heart of operations. Training, vendor management, safeguards – all are at the forefront. Phishing simulations, a Q&A forum, new hire training, to automated technology protection like vulnerability scans and intrusion detection, plus the physical and virtual safeguards are all part of the process. That includes operational controls like managing the status of employee computers. The organization also exercises external validation of operational processes using pen-testing and applying a table-top test of Business Continuity, Incident, and Disaster Recovery plans.

Kudos moment

The healthcare technology organization's COO shared a particular instance when the Apgar team's certification readiness expertise came to bear. It was during a series of auditor conversations about a specific control.

"Apgar & Associates helped us steer what was evolving into a confusing conversation that had the potential to result in an exception to SOC2 compliance. Just to navigate that discussion required experience depth we didn't yet have around Common Criteria and SOC2 control appropriateness to match the criteria. Their knowledge was invaluable in helping to bridge the gap between the auditor's understanding and our internal processes."

The healthcare technology company felt confident heading into the official SOC2 attestation process. They credit the partnership with Apgar & Associates for being in reach of the company's infosec goal within their projected timeframe.

According to the CEO, "From a headcount perspective, we're a small organization. Yet Apgar & Associates didn't see that as a barrier to developing a high-achieving infosec program. We never felt hampered or bogged down in costly practices while striving for this new level of excellence. They've been true partners throughout the various components of the engagement."

Apgar & Associates

Ready to take off on your path to certification?

Call Apgar & Associates today.

Their prep process, aka **certification readiness services**, have helped many organizations successfully achieve SOC 2, HITRUST, and ISO certifications.

503-384-2538
info@apgarandassoc.com

Julia Huddleston, CIPP / CIPM, CCFSP

Kevin Haralson, MBA, CCSFP, CHP