SOC & HITRUST – Answering Your Frequently Asked Questions

Jennifer Jones & Ryan Boggs / FORVIS

During a recent webinar, we discussed how SOC and HITRUST reports can help benefit your organization. Since we received several follow-up questions after the webinar, we compiled a “Frequently Asked Questions” document for you to download and keep on hand as you navigate through which report may best suit your organization’s needs.

SOC and HITRUST are two leading third-party assurance reports. What is your perspective on each, and how can organizations leverage each to meet their customer requirements?

SOC and HITRUST are leading third-party assurance reports that organizations can use to elevate and communicate their control environment to current and prospective customers. These reports are beginning to be a barrier to entry to work with some organizations. By utilizing these reports, organizations can increase their customer base by evidencing that the information they maintain, share, and store is protected.

SOC 1 reports focus specifically on meeting auditors’ expectations from a financial reporting perspective. Financial statement auditors place reliance on these reports when performing their audit. SOC 2 reports focus on the IT controls of organizations and are based on five trust categories. HITRUST is used predominantly in the healthcare space and has three separate assessment types: e1, an annual baseline assessment; and i1, an annual incremental assessment leading up to the r2 assessment, the flagship certification.

How have clients of FORVIS begun their SOC and HITRUST journeys?

Readiness Assessment – Based on increasing demands from customers, an organization worked with **FORVIS** to identify HITRUST as the most appropriate solution to meet its third-party assurance requirements. FORVIS developed a strategic road map through a phased approach to initiate the organization’s HITRUST journey. Initially, FORVIS evaluated policies and procedures to help ensure each document aligned with the HITRUST MyCSF requirements. Once policies and procedures were established and aligned, FORVIS verified that each requirement was implemented appropriately. This implementation Readiness Assessment included a test of each requirement to verify that the client maintained appropriate evidence to support a mature control environment. FORVIS consulted with members of management to help remediate each gap identified prior to beginning the next step, which was a HITRUST validation.

SOC 2 Transition to HITRUST – A legacy client of FORVIS began to identify the need to integrate HITRUST into its third-party assurance reports. Because of the client’s status as a current SOC 2 client of FORVIS with sound controls, FORVIS was able to perform a mapping exercise from the SOC 2 report to the HITRUST requirements to quickly outline the new controls that would need to be implemented. Though a Readiness Assessment aligned with the new controls, FORVIS quickly and effectively added HITRUST to the client’s third-party assurance program.

Assessor Transition **–** Our focus on client service allows the HITRUST assessor team to transition organizations efficiently and effectively to FORVIS as their preferred HITRUST assessor. This approach enables the organization to leverage a top 10 public accounting firm and our robust HITRUST team to perform future HITRUST certifications. Once selected as the assessor, FORVIS performs a detailed evaluation of the scope and approach currently utilized and consults on changes to provide a more efficient certification. FORVIS then works with management to outline a strategic plan to perform future HITRUST certifications while focusing on delivering an **Unmatched Client Experience**®.

Do clients feel there is an expectation gap from customers regarding what controls you execute on their behalf versus what they are responsible for?

Many vendors also have vendors; therefore, identifying the responsibility and ownership of a control can be a challenge. Through HITRUST, organizations can leverage an inheritance function to leverage other third parties' HITRUST certifications or SOC 2 reports within their own HITRUST certifications. This inheritance function can help clients leverage the controls and corresponding maturity from the third parties their organization utilizes. This approach can decrease the timing of HITRUST implementation and certification. The inheritance function also discloses to customers the use of third parties and helps enable customers to have confidence that the company maintains sound third-party risk management controls.

What does FORVIS suggest for organizations beginning their SOC and HITRUST journeys?

- Ensure that HITRUST provides strategic value;
- Obtain outside help to guide you through the process;
- Identify and educate your stakeholders, setting their expectations from a timeline perspective (timing is critical); and
- Define a reasonable and executable scope.

Tip: Strategically outline your HITRUST certification timing to align with slower times of year within your organization.

CSF v11 was a robust update to the HITRUST MyCSF. Why should I be an early adopter of CSF v11?

CSF v11 has created consistency and prescriptive tests for assessors. Organizations should consider adopting v11 if they are initiating their HITRUST certification process. By utilizing v11 from the onset of your implementation and certification, you can reduce the impact of migrating to this new version when it becomes required for all HITRUST certifications.

When an organization is considering a SOC examination or a HITRUST certification, how can they decipher which is best for them?

Organizations should evaluate contracts initially to determine what type of third-party assurance to pursue. Many contracts now incorporate a right-to-audit clause which can be reduced if an organization maintains a SOC report or HITRUST certification. Organizations may also benefit from a SOC report or HITRUST certification to reduce the burden of having to complete multiple security questionnaires from various customers. Many of these questionnaires can be reduced or eliminated if an organization maintains a SOC report or HITRUST certification. Once your organization identifies the type of report that provides the most strategic value, the scope of the report or certification should be determined. Many organizations initiating their third-party assurance approach should consider isolating the scope of the report or certification to those solutions that maintain Personally Identifiable Information (PII) or Protected Health Information (PHI). These solutions are usually the most material to customers.

What do you think organizations can expect in the coming years for HITRUST?

Currently, the focus of HITRUST assessments has shifted to implementation evidence which demonstrates that the organization maintains mature controls related to information security and data privacy. As the healthcare industry continues to rely on third parties for critical services, FORVIS expects HITRUST to increase its dominance as one of the most recognized and valuable certifications.

The rollout of the e1 and i1 certification has permitted organizations to implement HITRUST over a period of time. This phased approach allows organizations of all sizes and maturities to consider HITRUST for their third-party assurance reporting needs. FORVIS expects more organizations to utilize the e1 and i1 certifications to demonstrate their commitment to information security and data privacy while pursuing an r2 certification at some point in the future.

FORVIS also expects healthcare organizations to continue to leverage HITRUST as part of their third-party risk management approach. With HITRUST's e1 and i1 certifications, healthcare organizations can quickly compare third parties, as both certification types maintain a standard set of controls. In the future, we believe HITRUST will be leveraged extensively by healthcare organizations to assess the controls at third parties.

How are clients using SOC and HITRUST to tackle other compliance initiatives, such as state requirements and other compliance frameworks?

HITRUST's MyCSF tool should be utilized by organizations to assess compliance requirements outside of the e1, i1, or r2 certifications. The MyCSF tool enables organizations to perform internal assessments against a wide array of compliance requirements including, but not limited to, CCPA, GDPR, PCI, NIST, HIPAA, and other national and state compliance frameworks. By leveraging HITRUST's MyCSF tool to certify the organization and by also assessing new or potential compliance requirements, organizations are able to concentrate their compliance monitoring into a central solution. FORVIS encourages clients to leverage MyCSF and all of its capabilities to showcase this value proposition.

How can FORVIS support organizations with SOC and HITRUST?

We're here to help! We are big proponents of helping you review your strategic outlook and supporting you in selecting the best approach. We want to look ahead and help you answer questions such as, How will it meet your objectives? How can it help you grow? How can you be successful within the marketplace? There's a lot of time and resources put into a HITRUST assessment, so we're here to help you prepare. We want to help you look forward and continue your journey with SOC and HITRUST.