Deloitte.

SOC 2 for HITRUST

A complementary reporting option

By Chad Phillips, director, Finance & Operations Risk Transformation, and
Mark Ford, principal, Cyber Risk Services,
both within the Life Sciences and Health Care practice of
Deloitte & Touche LLP

What is a SOC 2?

A service organization controls (SOC) type 2 examination reports on the design, implementation, and operating effectiveness controls at a service organization to address the American Institute of Certified Public Accountants' (AICPA) Trust Services Principles and Criteria (TPA Section 100) related to security, availability, processing integrity, confidentiality, or privacy. A SOC 2 examination is similar in structure and general approach to the SSAE 16/SOC 1 reporting standard (legacy SAS70), but also allows the flexibility to incorporate additional suitable criteria, for example, around adherence to public industry-specific frameworks such as the HITRUST Common Security Framework (CSF).

Types of SOC Reports

SOC 1	SOC 2	SOC 3
SSAE16 — Service auditor guidance	**AT 101**	**AT 101**
Restricted Use Report (Type I or II Report)	Generally Restricted Use Report (Type I or II Report)	General Use Report (with public seal)
Purpose: Reports on controls for financial statement audits	**Purpose:** Reports on controls related to compliance or operations	**Purpose:** Reports on controls related to compliance or operations

SOC 2 Reports

Cover business areas outside of financial reporting, for example, security, privacy, processing integrity, availability or confidentiality

Can be applied for regulatory or non-regulatory purposes, across industries and business sectors

Can be distributed to user entities and specified parties

The five AICPA Trust Principles may, in turn, be mapped to the HITRUST CSF requirements:

- **Security** against unauthorized access or appropriation, either physical or logical
- **Availability** of operations
- **Processing integrity**, including complete, accurate, and timely processing
- **Confidentiality** of information
- **Privacy**, in keeping with AICPA's Trust Principles and the organization's privacy policy (e.g., personally identifiable information (PII) and confidential data) or other regulations

What is the HITRUST CSF?

"The CSF is a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management. It rationalizes healthcare-relevant regulations, standards, best practices and risk related events (such as cyber threats and breach data) into a single overarching security framework. Because the CSF is both risk- and compliance-based, organizations can tailor the security control baselines based on a variety of factors including organization type, size, systems, and regulatory requirements. By continuing to improve and update the CSF, it has become the most widely-adopted security framework in the U.S. healthcare industry." – Daniel Nutkis, CEO, HITRUST Alliance, LLC

Increasing demand for third-party internal control reporting

Cyber security is at the top of mind of management, boards, and regulators. With the impact of recent regulatory oversight such as the Department of Health and Human Services' (HHS) new Omnibus rules, organizations are under increasing pressure to demonstrate that they have taken appropriate measures to secure their environment; are vigilant in anticipating what might occur in the evolving security landscape and design detection systems to anticipate new threats, and are resilient in their ability to recover operations when a security incident does occur.

Health care entities and related business associates (e.g., health plans, health care clearinghouses, exchanges, health care providers, and organizations that conduct certain financial, research, and administrative functions) are being asked with increased frequency to demonstrate that they meet the common security and privacy requirements such as HIPAA Security & Privacy requirements, NIST, ISO, PCI and other standards. These entities are often replying to more than 200 individual audit requests, customer questionnaires, and security and privacy questions in response to request for proposals every year, many requiring a separate analysis and response to the same or overlapping questions. In addition, entities respond to these third-party requests in a multitude of forms and reporting formats. These requests may sound like the following:

"We need to see your…

…HITRUST Self-Assessment Report"

…HITRUST Verified Report"

…HITRUST Certified Report"

…SSAE16/SOC1 Report"

…responses to our questionnaire"

…documented processes and procedures"

…SOC 2 report"

Although HITRUST has worked within the healthcare industry to establish an industry accepted standard of reporting, various customers, some of which are outside the healthcare industry, request multiple reporting formats. Therefore, entities need to be prepared to efficiently respond to all types of requests. What is the answer? A SOC 2 report, mapped to the HITRUST CSF, may be crafted to reduce the number of customized reporting requests and be distributed to meet many requests by customers and other stakeholders. In support of this initiative, HITRUST and the AICPA are collaborating to align the Trust Principles to the HITRUST CSF, which will provide a standard and comparable reporting framework for use in SOC 2 reporting.

I thought HITRUST would meet my third-parting reporting needs

HITRUST has developed a standard report that provides a consistent representation of risk exposure, compliance posture and corrective actions that allow for benchmarking of results against security practices at similar organizations in the industry. However, as noted previously, requests come in for other reporting attributes, such as response to security questionnaires, requests for proposals, description of processes and controls implemented to satisfy the CSF, and assurance that controls operated as designed for a fixed and continuous period of time (a rolling six- or twelve-month reporting cycle). Therefore, the HITRUST reporting model and the SOC2 reporting model are complementary since both are facilitated through the efficient assessment and implementation of controls to satisfy the CSF.

The benefits of a converged reporting model

For decades, the AICPA has been the recognized professional body for providing assurance around both financial reporting and outsourced operations. Incorporating HITRUST with an AICPA recognized reporting model strengthens the framwork's impact to the marketplace. Benefits include the following:

- Extends the AICPA's recognized standard for assurance around financially significant outsourced services (SSAE 16/SOC 1) to operational areas of interest to your customers (SOC 2)
- Offers significant time efficiencies and cost savings due to the overlap between the CSF controls and Trust Principles
- Reduces the burden of multiple control frameworks and reporting requirements
- Provides one broad, scalable and up-to-date framework that is relevant to their organization and may be leveraged to meet the wide and varied array of information protection requirements

Benefits to report issuers:

- **Save on time and costs** — Reduces time spent by internal resources in responding to multiple redundant individual requests. Decreases the number of individual audits that your organization undergoes
- **Feel the synergy** — Gains efficiencies by implementing a SOC 2 report that leverages the work invested in the HITRUST CSF implementation
- **Increase customer satisfaction** — Increases ability to provide a customer the information that they want in the format they desire

Benefits to report recipients:

- **Meets your varied requests** — Whether requesting a HITRUST report, SOC 2 report, or mapping a SOC 2 to your format, a report will be available to meet your needs
- **Recognizes a standard in assurance reporting** — Alignment with recognized AICPA reporting formats allows for streamlined adoption of a SOC 2 for HITRUST report within a recipient's existing internal control monitoring processes

Where do you go from here?

The most important step in assessing your internal control position in response to third-party internal control reporting is to fully understand the specific risks faced by each third-party constituency (e.g., customers, potential customers, regulators, business associates). Understanding the specific operations, regulatory, and compliance needs of each of these constituencies will allow your organization to determine the context of the third-party reporting requests you receive, evaluate the nature and extent of controls that need to be demonstrated to satisfy those requirements, and determine the most efficient and effective method(s) of internal control reporting.

Determine the context of the third-party reporting request:
Within the context of this article, third-party requirements for HIPAA compliance are clear. However, depending upon the type of business third-parties are in, and the services that your organization provides, other requirements could be in play. These could include Payment Card Industry (PCI) compliance, federal standards such as the Federal Information Security Management Act (FISMA), or service level agreements, as examples.

Evaluate the nature and extent of controls to meet identified requirements:
As a reader of this article, you either have adopted, or have interest in adopting, the HITRUST CSF. This framework provides a foundation on which your organization can identify and map internal controls. The HITRUST CSF is a rationalized control set which allows organizations to map to a single framework knowing that multiple regulatory standards will, by extension, be satisfied (e.g., HIPAA, ISO, FISMA). For those standards not already mapped to the HITRUST CSF, but identified as relevant based upon your third-party risk assessment, you can identify controls to meet those specific needs.

The extent of your internal control deployment will be focused, at a minimum, on those systems and processes that support your third-party services. Clearly defining the boundaries of your system subject to the HITRUST CSF will prevent “scope creep,” — or extending controls to systems that may not be relevant to third-parties—will allow for a focused evaluation of third-party risk mitigation, and will contain the costs of your internal control initiative.

Determine the most efficient and effective method(s) of internal control reporting:
Knowing that some third-parties will have very specific reporting formats that you will not be able to deviate from, it is important to implement a third-party internal control reporting structure that is efficient, yet flexible. Mapping the HITRUST CSF to the AICPA Trust Principles used in SOC 2 reporting is a way to provide that efficient and flexible structure. Under this structure of reporting, the SOC 2 for HITRUST report becomes the default method of reporting to meet the widest range of requests.

The SOC 2 report would include an opinion from a registered AICPA CPA firm with regard to the design, implementation, and operating effectiveness of controls, a written assertion from your organization’s leadership regarding your commitment to your internal control practices, a description of the internal control practices you have deployed against the HITRUST CSF, the test procedures and results of testing performed by the CPA firm, and management’s corrective action plan aligned to the control exceptions identified.

For those third-parties wanting to determine your maturity against the HITRUST CSF, HITRUST has available reporting under self-assessment, validated, or certified reports. In the case of HITRUST validated or certified reports, you can engage a CPA CSF Assessor, thereby gaining the efficiency of testing once to satisfy both HITRUST and SOC 2 reporting needs.

Lastly, for those third-parties requiring specific responses in their pre-defined format (e.g., security questionnaires), you can map your SOC 2 for HITRUST controls as responses to specific questions the third-party may be requesting, with the full SOC 2 report as a supporting reference document.

The graphic below illustrates the various reporting methods available to your organization under a SOC 2 for HITRUST reporting model, each of which is leveraged off of the Trust Principals/HITRUST CSF mapping foundation.