SOC 2 Audits & HITRUST CSF Assessments

As a tending organization – or supplier of services to the broader tending arena – you've most likely stumble upon the SOC 2 HITRUST topic. After all, in today's world of ever-growing regulative compliance mandates, SOC 2 HITRUST is currently front and center for thousands of companies throughout North America.

And with HITRUST certification comes on one in every of the most important queries that tending organizations area unit asking themselves: Should we tend to become HITRUST CSF compliant, or have a certified public accountant firm perform a SOC 2 HITRUST assessment on my organization, and what's the difference?

Let's examine this in additional detail.

- What is HITRUST?
- What is SOC 2?
- What area unit the variations Between SOC 2 and HITRUST?
- When combined, what's a SOC 2 HITRUST Report?
- Tips in getting ready for SOC 2 HITRUST
- The Importance of Policies and Procedures for SOC 2 HITRUST

What is HITRUST?

According to https://hitrustalliance.net/, HITRUST, in conjunction with personal sector, government, technology and data privacy and security leaders, has developed the HITRUST CSF, a certifiable framework that may be employed by any organization that makes, accesses, stores or exchanges sensitive info.

Furthermore, the HITRUST CSF harmonizes multiple frameworks, standards, state, federal and International laws and leading practices into one framework. The HITRUST CSF addresses industry-specific challenges by investment and enhancing existing frameworks, standards and laws to supply organizations of variable sizes, geographic operation and risk profiles with prescriptive implementation necessities and pointers.

Lastly, the HITRUST CSF may be a climbable, prescriptive and certifiable framework that harmonizes varied standards, laws, management frameworks and leading practices.

Specifically, HITRUST CSF Certification needs the services of a HITRUST approved CSF tax assessor organization. The result's a report with findings that may incline to customers, prospects, local/state/federal agencies, and alternative applicable entities.

What is SOC 2?

SOC 2 – System associated Organization Controls (SOC) – is an auditing framework place forth by American Institute of Certified Public Accountants for auditing service organizations. Important to the SOC 2 framework are the following Trust Services Criteria (TSC):

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

Specifically, in keeping with the AICPA, SOC 2 reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

More merely expressed, SOC 2 audits (mainly – a SOC 2 Type 1 and a SOC 2 Type 2) effectively assert on whether or not the controls were designed properly (Type 1) and/or such controls operated effectively (Type 2) in accordance with the necessities place forth by the applicable trust services criteria and therefore the connected common criteria.

As expressed earlier, there 5 trust services criteria (TSCs) that a service organization (i.e., your business) will be assessed against during a SOC 2 audit: security, availability, processing integrity, confidentiality, and privacy. The security TSC is required for the SOC 2 audits, with the remaining four deemed optional, but can be added depending on the service provided.

It's vital to recollect that SOC reports are well-known within the world of auditing, and as a result, will meet a wide-range of control compliance news for varied industries. So, along comes HITRUST and currently the choice of getting a SOC 2 HITRUST report, one thing that creates sense for the massive variety of tending organizations throughout North America. Let's take a glance currently at what precisely SOC 2 HITRUST is.

Differences between SOC 2 and HITRUST?

Technically speaking, the most important distinction is that SOC 2 is associate AICPA "attestation" report, whereas HITRUST may be a "certification" report. Additionally, the "attestation" side of SOC 2 compliance means management (i.e., the service organization that the SOC report is being performed on) attests to the data contained among the particular SOC 2 report. In addition, the freelance auditor (i.e., certified public accountant firm) ultimately confirms the attestation via associate opinion letter.

Now, there is totally different "opinions" issued by the certified public accountant firm, like "unqualified", that may be a clean report, or "qualified" or "adverse", that is mostly seen as associate adverse or suspect report on one's control surroundings.

As for HITRUST, again, it's a certification, and is undoubtedly a far detailed report as compared to a typical, baseline SOC report. The HITRUST CSF framework has additional controls, additional detail, and additional overall testing necessities than a typical, baseline SOC 2. This ultimately needs longer and energy from businesses undergoing HITRUST CSF compliance.

Keep in mind that HIRTUST has engineered the particular CSF framework from a range of standards – with a significant stress from ISO 27001/27002 – and therefore the result's a collection of controls so much larger than a typical, baseline SOC 2.

Combined SOC 2 HITRUST Report?

A SOC 2 HITRUST report is basically a SOC 2 combined with the HITRUST CSF management necessities used because the basis of associate organization's cyber security and data framework. To support this approach, HITRUST and therefore the AICPA have collaborated to align the Trust Services Principles and Criteria to the HITRUST CSF that provides customary and comparable necessities to be used in SOC 2 report. Note that only an Certified Public Accountant (CPA) firm will issue a SOC 2 HITRUST.

Tips in getting ready for SOC 2 HITRUST

One of the fundamentally most important measures any service organization can do in preparing to undergo an initial SOC 2 HITRUST assessment is to perform a scoping & readiness assessment. You'll need to asses and identify certain scoping issues, such as what information systems, personnel, physical locations, third-party providers – and more – are in scope. Second, you'll want to identify gaps and deficiencies within your control environment that require remediation, such as policies and procedures, technical/security misconfigurations, and more.

We believe, that the article what have enhance your understanding of the two standards and their key differences. Please reach out us if you still have any queries or for any further information.