HITRUST

Providing Reliable Assurances

Understanding the Differences Between a HITRUST CSF® Assessment Report and an AICPA SOC 2® Report

Organizations have many options when it comes to assessing and reporting upon their information security and privacy posture; however, not all provide the same level of reliability. The level of assurance needed is different for every business relationship, dependent upon the level of risk posed by the relationship. For some, an AICPA SOC 2 may be acceptable; others may require more reliable assurances, such as a HITRUST CSF Assessment Report.

There are many criteria that organizations should consider when evaluating the reliability of a control assessment and reporting framework, six of which are key: transparency, scalability, consistency, accuracy, integrity, and efficiency. While the AICPA SOC 2 framework and examination report have specific uses and can provide value, they do not fully address several of these criteria, specifically transparency, accuracy, integrity, and efficiency.

Transparency

With HITRUST CSF Validated Assessment Reports, the HITRUST CSF control framework is publicly available and changes are documented extensively in every release. HITRUST's robust assessment approach, control maturity and scoring methodology, and related assurance requirements are also clearly articulated in publicly available guidance.

SOC 2 is a reporting framework rather than a control framework and thus does not provide the controls needed to achieve the criteria specified by the AICPA Trust Services Criteria (TSC). While an AICPA SOC 2 report may specify the controls used to evaluate each of the TSC within the scope of the report, information on the controls and how they were selected are only made available to recipients of the report rather than the public at large. Additionally, while the approach used to evaluate the controls follows AICPA standards, the specific methods used can vary from one CPA firm to another.

Accuracy

HITRUST provides the only assessment report that clearly articulates control maturity using its innovative PRISMA-based, quasi-quantitative control maturity and scoring model, lending a degree of accuracy simply not achievable by traditional assessment approaches, i.e., yes/no.

To read more about the importance of assessing control maturity when providing assurances, read our white paper, *Evaluating Control Maturity Using the HITRUST Approach*.

Integrity

The HITRUST CSF Assurance Program, governed by a Quality Assurance Subcommittee of its Board of Directors, overseen and audited by a Compliance department, and managed by an Assurance department, provides a granular level of oversight through a quality control process that reviews each assessment and resulting report it produces. Today, each assessment submitted by a HITRUST Authorized External Assessor undergoes over four dozen automated quality checks to identify and address assessment errors and omissions; in addition, each assessment is handed off to Quality Assurance Analysts within HITRUST's Assurance team for review. The work of the Assurance team is continuously audited by the Compliance team, and quality metrics are reported quarterly to the Board's Quality Assurance Subcommittee, bi-weekly to the HITRUST CEO, and weekly to the Assurance team's leadership. Any problems with assessments introduced by assessors are quickly identified and corrective actions taken.

>>>

The AICPA's attestation standards require CPA firms to perform limited internal reviews and periodic peer reviews of SOC engagements. However, no reporting option other than HITRUST provides centralized management and oversight of each and every assessment performed by its assessors.

Efficiency

Since HITRUST has harmonized various relevant information risk and compliance frameworks, best practices, and regulations into a single set of rationalized control requirements, organizations that leverage HITRUST do not need to answer more questionnaires or conduct more assessments than absolutely necessary. And because HITRUST also supports transparency, scalability, consistency, accuracy, and integrity in its assessment and reporting process, it is able to deliver a single, comprehensive assessment report that can provide appropriate assurances for multiple requesting parties, saving organizations significant time and money—an approach HITRUST calls *Assess Once, Report Many*™.

As the SOC 2 is a reporting framework, the AICPA does not specify the controls needed to achieve the trust services criteria included in the report. Although SOC 2 reports do not inherently address a control framework other than the one used, if any, to provide the controls needed to address the criteria included in the report, information regarding their relationship to other frameworks could be included in a section titled 'unaudited information'.

While organizations have many options for assessing and reporting upon their security and privacy programs, HITRUST provides the most reliable assurances to stakeholders that an organization is properly addressing information risk management and compliance concerns. To learn more, read our data sheet, *What Makes an Assurance Report Rely-able?*

Criterion	Assessment Reporting Option Attribute	AICPA SOC2	HITRUST CSF
Transparency	Open Controls Framework	N/A[1]	Yes
	Open Assessment Methodology	Yes[2]	Yes
Scalability	Tailorable Controls Framework	N/A	Yes
	Market-based Assurance Program	Yes	Yes
Consistency	Prescriptive Control Assessment Methodology	Yes[3]	Yes
	Trained, Vetted Assessor Pool	Yes[4]	Yes
Accuracy	Maturity-based Implementation Model	No	Yes
	Quasi-quantitative Scoring Approach	No	Yes
Integrity	Formal Assessor Program	Yes[5]	Yes
	Centralized Quality Assurance	No	Yes
Efficiency	Integrated & Harmonized Control Framework	N/A[6]	Yes
	Standardized Report w/ Optional Scorecards	Yes[7]	Yes

1 SOC 2 is a reporting framework rather than a control framework; it does not provide the controls needed to achieve the outcomes specified by the AICPA TSC.

2 AICPA (2018, Jan 1). *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.* Chicago: Author.

3 AICPA (2018, Jan 1). *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.* Chicago: Author.

4 AICPA SOC 2 engagements are performed by CPAs via CPA firms.

5 SOC 2 reports must be signed by a CPA and follow AICPA standards.

6 SOC 2 is a reporting framework, and AICPA does not specify the controls needed to address the objective-level Trust Services Criteria used in the report.

7 Although SOC 2 reports do not inherently address a control framework other than the one used, if any, to provide the controls needed to address the TSC used in the report, this information regarding their relationship to other frameworks could be included in a section titled 'unaudited information' in an appendix.