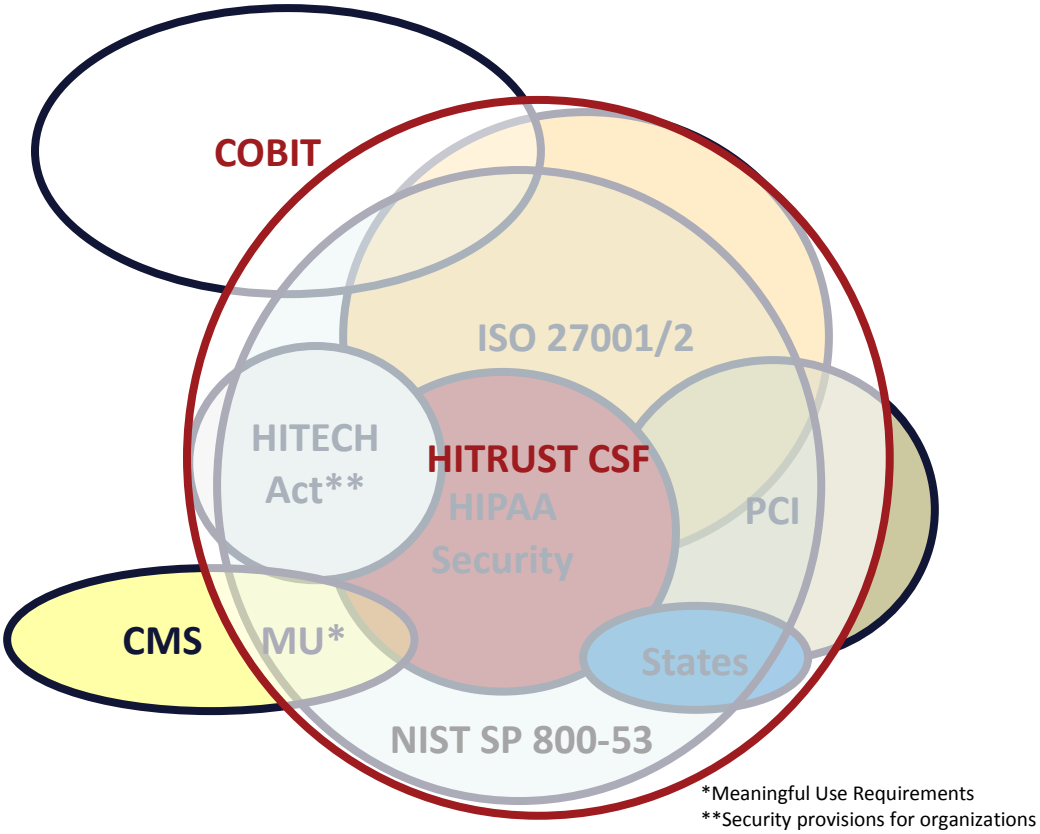
INTRODUCTION

Overview

The Health Information Trust (HITRUST) Alliance, the organization responsible for the development of the HITRUST Common Security Framework (CSF), and the AICPA have collaborated to develop and publish a set of recommendations to streamline and simplify the process of leveraging the HITRUST CSF and CSF Assurance programs for SOC 2® reporting.[1]

HITRUST Background

HITRUST was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST—in collaboration with health care, business, technology, and information security leaders—has established the HITRUST CSF, a certifiable framework that can be used by all organizations that create, access, store, or exchange personal health and financial information. Beyond the establishment of the HITRUST CSF, HITRUST is also driving the adoption of (and widespread confidence in) the framework and sound risk management practices through awareness, education, advocacy, and other outreach activities. Visit www.HITRUSTalliance.net for more information about HITRUST, the HITRUST CSF, and other HITRUST offerings and programs.



[1] SOC: Service organization controls.

HITRUST CSF

An integral component to achieving HITRUST's goal to advance the health care industry's protection of health information is the establishment of a practical mechanism for validating an organization's compliance with the HITRUST CSF.

The HITRUST CSF is an overarching security framework that incorporates and leverages the existing security requirements that health care organizations must comply with, including requirements of federal (for example, HIPAA and HITECH), state, third party (for example, PCI and COBIT), and other government agencies (for example, NIST, FTC, and CMS). The HITRUST CSF is already being adopted by leading health care payers, providers, and state exchanges as their security framework.

HITRUST has developed the CSF Assurance program, which encompasses the common requirements, methodology, and tools that enable both health care organizations and their business partners to take a consistent and an incremental approach to managing compliance.

HITRUST CSF Certification

HITRUST operates a program in which approved HITRUST CSF assessors perform an assessment of an organization in connection with the organization's application for HITRUST CSF certification. HITRUST evaluates the results of the work performed by the CSF assessor to validate the organization's assessment. HITRUST makes a determination about whether the organization meets the CSF requirements and then issues a HITRUST certification report if the organization meets the requirements.

SOC 2 + HITRUST CSF Reporting Options

A mapping between the requirements of HITRUST CSF version 7 and the criteria for the security, availability, and confidentiality principles included in the AICPA's Trust Services Principles and Criteria (applicable trust services criteria) has been developed and made available to enable service organizations to provide information to users of the service organization's system about whether controls at the service organization relevant to security, availability, and confidentiality are suitably designed and operating effectively to meet the applicable trust services criteria and the HITRUST CSF requirements. This enables the service organization to communicate information about the processes and procedures it uses to meet the HITRUST CSF in addition to the applicable trust services criteria, increasing transparency and information for decision making.

Service organizations may wish to consider the following four options for reporting:[2]

1. SOC 2 reporting only—This option is used when a service organization does not choose to have its service auditor express an opinion on whether the controls at the service organization are suitably designed and operating effectively to meet the HITRUST CSF.

[2]Except for option 3, HITRUST CSF certification (without a SOC 2 report), these options are performed by a CPA under the AICPA's Statements on Standards for Attestation Engagements (attestation standards).

It provides the service organization with a service auditor's examination report that includes an opinion on the fairness of the presentation of the description, based on description criteria in the AICPA SOC 2® guide,[3] and an opinion on the suitability of the design and operating effectiveness of the controls based on only the applicable trust services criteria. The report does not include an opinion on whether the controls were suitably designed and operating effectively based on the HITRUST CSF requirements. (Service organizations may include a mapping of the HITRUST CSF requirements to the applicable trust services criteria in section 5 [unaudited section] of the SOC 2 report to provide additional information for report users.)

2. SOC 2 + HITRUST CSF reporting—This option is used when a service organization wants its service auditor to express an opinion on whether the controls at the service organization are suitably designed and operating effectively to meet the HITRUST CSF requirements in addition to the applicable trust services criteria. It provides the service organization with a service auditor's examination report that includes
    - an opinion on the fairness of the presentation of the description based on the description criteria in the AICPA SOC 2® guide and
    - an opinion on the suitability of the design and operating effectiveness of the controls based on
        - the applicable trust services criteria and
        - the HITRUST CSF requirements.
3. HITRUST CSF certification (without a SOC 2 report)— This option is used when a service organization wants to provides its stakeholders with a HITRUST CSF certification report but does not choose to provide them with a SOC 2 report. This engagement is performed by an approved HITRUST CSF assessor based on the HITRUST CSF requirements. That assessor may be, but is not necessarily, a CPA. The engagement consists of an assessment that is submitted to HITRUST for evaluation and, if the service organization's controls meet the HITRUST CSF requirements based on a determination by HITRUST, the issuance of a certification report by HITRUST.
4. SOC 2 + HITRUST CSF + CSF certification—This option is used when a service organization wants its service auditor to express an opinion on whether the controls at the service organization are suitably designed and operating effectively to meet the HITRUST CSF requirements in addition to the applicable trust services criteria and to provide its stakeholders with a HITRUST CSF certification report. It provides the service organization with a service auditor's examination report that includes an opinion on the fairness of the presentation of the description, based on the description criteria in the AICPA SOC 2® guide, and an opinion on the suitability of the design and operating effectiveness of the controls based on (1) the applicable trust services criteria and (2) the HITRUST CSF requirements. In addition, the service organization may include its HITRUST CSF certification report (refer to option 3 discussed previously) in section 5 (unaudited section) of its SOC 2 report. Typically, the service auditor and the approved

[3] The fairness of the presentation of the description is based on the description criteria in the AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (SOC 2® guide)

HITRUST CSF assessor are the same organization and the tests performed and results of tests performed by the service auditor or approved HITRUST CSF assessor (or both) are used by HITRUST as a portion of the basis for the HITRUST certification.

The use of a SOC 2 engagement enables health care and other organizations to communicate information about their programs for complying with HIPAA or other regulatory requirements in a single report that provides information about the organization's controls over protected health information (PHI) based on the applicable trust services criteria and the HITRUST CSF requirements. This provides service organizations with the ability to increase transparency and communicate through a single deliverable to customers, business partners, and stakeholders both in and outside the health care sector.

Key References

The following resources may be helpful in understanding the types of engagements and resulting reports discussed in this paper: AT section 101, *Attest Engagements* (AICPA, *Professional Standards*); AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)*; HITRUST CSF; HITRUST CSF Assurance Program Requirements; HITRUST Assessment Methodology; and Risk Analysis Guide for HITRUST Organizations and Assessors.

HITRUST CSF and HITRUST CSF Certification

As previously described, HITRUST has developed and published the HITRUST CSF and the HITRUST CSF certification program.

Q: Is a HITRUST CSF certification a reporting option under AICPA attestation standards?

A: No. HITRUST CSF certifications are issued by HITRUST based on policies and guidelines it has established. HITRUST administers the program in which assessments are performed and HITRUST CSF certification reports are issued.

Q: Is a HITRUST CSF certification part of SOC 2 + HITRUST CSF engagement?

A: No. The information in a service auditor's report resulting from a SOC 2 + HITRUST CSF engagement may be used by service organizations as input to the HITRUST CSF certification process, but does not equate to a HITRUST CSF certification. The HITRUST CSF certification report is separate and distinct from any deliverable issued under AICPA guidance. The HITRUST CSF contains specific requirements, which in most situations satisfy the requirements for suitable criteria as specified in AT section 101 and may be used in the performance of an attestation engagement under AT section 101. The use of the HITRUST CSF requirements as suitable criteria in an attestation engagement performed under AT section 101 is not equivalent to a HITRUST CSF certification.

Q: As a CPA, how can I assist an organization that wishes to obtain HITRUST CSF certification?

A: Approved HITRUST CSF assessors can perform an assessment of an organization's controls in connection with the organization's application for HITRUST CSF certification. A CPA may perform such an assessment under the AICPA's consulting standards, agreed-upon procedures, attestation standards, or other guidance, as deemed appropriate by that firm. HITRUST evaluates the results of the work performed by the assessor to validate the organization's self-assessment and determines whether a HITRUST CSF certification should be issued. The CPA will also need to be approved by HITRUST as a CSF assessor and adhere to HITRUST's rules relating to assessments and certifications (contact www.HITRUSTalliance.net for further information).

Q: Should the maturity of control attributes (for example, the HITRUST maturity characteristics of measured and managed) be assessed when performing a SOC 2 + HITRUST CSF engagement?

A: Service organizations can provide more details with respect to the measured and managed characteristics of the controls within the system description. This will provide increased transparency for users and HITRUST to assist them in evaluating maturing of controls.

SOC 2 + HITRUST CSF, SOC 2 + HITRUST CSF + CSF Certification Options

The SOC 2 + HITRUST and SOC 2 + HITRUST CSF + CSF certification options are engagements that a service auditor performs and reports on under AT section 101 and the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (SOC 2® guide). The reports resulting from these engagements include three opinions: (1) an opinion on the fairness of the presentation of the description based on description criteria in the SOC 2® guide, (2) an opinion on the design and operating effectiveness of the controls based on the applicable trust services criteria, and (3) an opinion on the design and operating effectiveness of the controls based on the HITRUST CSF requirements. A report on a SOC 2 + HITRUST CSF engagement could be either a type 1 report (which covers the fairness of the presentation of the system description and suitability of the design of the controls as of a date) or a type 2 report (which covers the fairness of the presentation of the system description, the suitability of the design of the controls and the operating effectiveness of the controls through a period of time); a SOC 2 + HITRUST CSF + CSF certification could be issued only as a type 2 report.

Q: Who is the responsible party?

A: Typically management of the service organization is responsible for the controls relating to PHI.

Q: What is the subject matter?

A: The service organization's description of its system, the suitability of the design of the controls relevant to PHI, and (in a type 2 engagement) the operating effectiveness of those controls.

Q: What are the suitable criteria?

A: There are two sets of suitable criteria. The criteria for security, availability, and confidentiality in the AICPA's Trust Services Principles and Criteria comprise one set of suitable criteria. The second set of suitable criteria consists of the HITRUST CSF requirements based on the service organization's characteristics per HITRUST's Organizational Factors (for example, sector, size, and complexity).

Q: One of the requirements of an attestation engagement under AT section 101 is that the criteria used to assess the subject matter be suitable. Does the HITRUST CSF meet the definition of suitable criteria as defined by the AICPA?

A: Yes. The practitioner must have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users. Criteria are the standards or benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. Suitable criteria must have each of the following attributes:

• Objectivity—Criteria should be free from bias.
• Measurability—Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
• Completeness—Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
• Relevance—Criteria should be relevant to the subject matter.

Criteria that are established or developed by groups composed of experts that follow due process procedures, including exposure of the proposed criteria for public comment, are ordinarily considered suitable. The CSF has been developed by HITRUST in collaboration with health care and information security professionals following due process that includes a comment process and therefore meets the requirements for suitable criteria.

The criteria are made available to the users of the report as disclosed in the SOC 2 HITRUST CSF report.

MAPPING

The mapping of the HITRUST CSF requirements to the criteria in the Trust Services Principles and Criteria is provided to help service auditors achieve efficiencies by designing audit procedures that enable the service auditor to evaluate controls based on both sets of criteria. The use of the mapping should reduce inefficiencies that could occur if one set of audit procedures was designed and executed for the HITRUST CSF and an entirely separate set of audit procedures were designed and executed for the Trust Services Principles and Criteria.

Q: Is inclusion of the mapping mandatory in a SOC 2 + HITRUST CSF report?

A: Although inclusion of the mapping is not required, use of the mapping is highly recommended. The mapping identifies the HITRUST CSF requirements that are closely aligned with the applicable trust services criteria. By using the mapping, it may be possible for the service auditor to design and perform tests that provide evidence about whether the service organization's controls are operating effectively to achieve the applicable trust services criteria and the related HITRUST CSF requirements. By leveraging the mapping, it is believed that significant efficiencies may be achieved in planning and performing this engagement and that the report will enable report users to obtain information about the service organization's controls through the lenses of both sets of criteria (Trust Services Principles and HITRUST CSF requirements).

Consideration should be given to identifying the controls (and tests of controls) that meet the criteria defined by both the applicable trust services criteria and the HITRUST CSF requirements. The mapping is a practice aid developed for this purpose.

Q: Which trust services criteria have been mapped to the HITRUST CSF requirements?

A: The criteria for the security, availability, and confidentiality principles have been mapped to the HITRUST CSF requirements. The mapping of the privacy criteria to the HITRUST CSF requirements is slated for a future release.

REPORTING

Q: Is the SOC 2 + HITRUST CSF report the preferred method for demonstrating HIPAA compliance?

A: The SOC 2 + HITRUST CSF report does not provide an opinion on HIPAA compliance. It is one of several options that provides information about controls related to HIPAA safeguards that may be helpful to user entities. The circumstances surrounding the services provided by the service organization should be considered when determining the most appropriate reporting option. However, the SOC 2 + HITRUST CSF report provides significant value to user entities by providing relevant descriptive information and an opinion on the design and operating effectiveness of a service organization's controls based on both the applicable trust services criteria and the HITRUST CSF requirements.

Q: How are exceptions addressed in a SOC 2 + HITRUST CSF report?

A: Any test exceptions are presented adjacent to the service organization's control, the corresponding applicable trust services criteria, and the HITRUST CSF requirement. The service auditor should consider the effect of all testing exceptions (deviations) on both sets of criteria. If the control deviations result in a modified opinion, it would also be disclosed in the relevant section of the opinion(s).

Q: In a SOC 2 + HITRUST CSF report, how does a modified opinion related to the applicable trust services criteria affect the opinion related to the HITRUST CSF requirements and vice versa?

A: During planning, the service auditor should identify the relevant service organizations controls that meet the criterion or criteria of the applicable trust services criteria and the HITRUST CSF requirements. If testing indicates that a service organization's control does not meet those criteria (in combination with complementary user entity controls), all criteria associated with the control would not be met. This is true regardless of which of the two sets of suitable criteria the criteria are associated with.

OTHER CONSIDERATIONS

Q: Can any CPA issue a SOC 2 + HITRUST CSF report or a SOC 2 + HITRUST CSF + CSF certification report? Must the CPA also be an approved HITRUST CSF assessor to perform either a SOC 2 + HITRUST CSF engagement or a SOC 2 + HITRUST CSF + CSF certification engagement?

A: In accordance with AT section 101.21–.22, the practitioner must have adequate knowledge of the subject matter. HITRUST offers specific training courses to practitioners interested in performing HITRUST engagements. As noted in the next question, the HITRUST CSF is the intellectual property of HITRUST and use of that intellectual property is subject to licensing requirements established by HITRUST, including the use of the HITRUST CSF framework. As also noted in previous Q&As in this document, the HITRUST CSF certification process requires that the assessment be performed by an approved HITRUST assessor.

Q: Are there licensing considerations when a CPA uses the HITRUST CSF in an engagement, including a SOC 2 + HITRUST CSF engagement?

A: Yes, the HITRUST CSF is the intellectual property of HITRUST. HITRUST makes the HITRUST CSF available online for free download subject to certain terms and conditions. These terms and conditions permit download of the HITRUST CSF by a user of a SOC 2 + HITRUST CSF report. However, use of the HITRUST CSF framework by a professional service firm or professional in connection with the provision of services (or both), including use as a part of a SOC 2 + HITRUST CSF engagement, requires the professional service firm or professional (or both) to obtain a license from HITRUST. The practitioner should contact HITRUST at sales@hitrustalliance.net or by phone (1.855.HITRUST or 1.855.448.7878) to inquire about available licensing options.