Third Party Assurance FAQ

1603 - v1.2

How can I use the CSF Assurance Program for third party risk management?

The CSF Assurance Program is specifically designed to streamline the third party risk management process by using a single comprehensive framework harmonizing multiple standards and best practices to support a single assessment that may be reported out in multiple ways, e.g., to support PCI SAQ development, the issuance of SOC 2 reports against specific AICPA Trust Services Principles, or scorecards of HIPAA or NIST Cybersecurity Framework compliance. Organizations using the CSF Assurance Program for third party risk management experience significant reductions in cost and level of effort required to evaluate third party reports or issue their own reports to their own stakeholders, including business partners and regulators. In short, the CSF Assurance program allows organization to focus on execution and results without having to worry about developing and maintaining an acceptable process or content. This is the fundamental reason why several large healthcare entities have moved from simply accepting HITRUST validated and certified reports to requiring them. To learn more about this recent announcement from several large healthcare entities, please click *here*.

References:* ***Managing Third Party Compliance* *or* ***CSF Assurance Program***

How much does it cost to get a HITRUST CSF certification cost?

Certification requires an organization to undergo a validated assessment, which basically means a qualified organization, specifically a CSF Assessor, needs to conduct an assessment leveraging the CSF Assurance program. There are two costs, the assessor costs – which are determined by the assessors, and the validated assessment report fee due to HITRUST. The report fee is based on your annual revenue and ranges from $3,750 to $7,500. Please note, most organizations choose to complete a self-assessment prior the validated assessment as part of a readiness assessment.

Additional information on comparable costs can be found in the FAQ: *Is a HITRUST certification assessment more expensive than comparable assessments?*

To find out the assessment fee for your organization, please contact *sales@hitrustalliance.net* or call 855-HITRUST.

How often do I need to get a report?

HITRUST CSF reports with Certification are valid for two years given the successful completion of an interim review, no breach has occurred and no significant changes have occurred relating to the scoped control environment. However, check with your business partner to ensure this meets their requirements as well.

Reference:* ***CSF Assurance Program Requirements*

How many questions, and how long will it take?

The HITRUST CSF Security Assessment Questionnaire generally includes between 120 and 328 questions, depending on how the risk factors are configured for the organization being assessed. The amount of time it will take to complete the assessment varies depending on the amount of time and resources available.

Reference:* ***HITRUST CSF Assessment Process*

How do I understand the CSF Assessment report I have received?

HITRUST has created a document that explains the assessment report, how to interpret, and how it can be used to compliment and enhance your current processes.

Reference:* ***Leveraging HITRUST CSF Assessment Reports: A Guide for New Users*

What types of questions are there, and what information will we need to provide?

The HITRUST CSF Assessment questionnaire will ask about your organization's information security practices in 19 major topical domains such as information protection program, endpoint protection, portable media security, third party assurance and risk management.

To gain an understanding of your organization's risk profile, the questionnaire will ask you if:

1. Specific requirements are addressed in organizational policy and standards,
2. There are processes and procedures to support the implementation of the requirements,
3. The requirements have been implemented consistently across the organization,
4. The effectiveness of the controls are monitored (e.g., with a metric or other type of measurement), and
5. The controls are actively managed based on this monitoring.

References:* ***HITRUST CSF Assessment Process*, ***CSF Assurance Program Requirements*** *and* ***Risk Analysis Guide***

Can I provide my ISO 27001 certification in lieu of CSF certification for third party assurance?

Organizations accepting ISO 27001 in lieu of CSF certification must still go through the traditional and demonstrably laborious process of comparing and contrasting what's in the ISO report with what it expects from the comprehensive, prescriptive and often granular requirements of the CSF. While an improvement over custom assessment questionnaires and the now legacy SAS 70, the relying organization would still need to identify any gaps between the two reports (which will almost surely exist), go through the process of requesting additional information from the ISO-certified entity, and then evaluate the response(s). While an organization could conceivably support ISO certification as a 'first step" in the assurance process, it could not and should not rely solely on ISO certification. At some point the ISO-certified organization must demonstrate that the complete set of CSF control requirements relevant to their organization have been implemented appropriately if it is to ascertain what residual risk(s) remain. And since this is best accomplished through the CSF Assurance Program, it just makes sense—from both an economic and resource perspective—to simply require a CSF validated or certified assessment from the onset.

References:* ***Risk Management Frameworks*, ***CSF Assurance Program Requirements*** *and* ***Risk Analysis Guide***

Is a current SOC2 acceptable for meeting the third party assurance requirements?

It depends. The accepting organization will need to make a determination based on the scope of the review and the trust principals involved. While the current SOC2 may be granted a waiver and accepted in the first year, it will be necessary to base future SOC2 reports on the HITRUST CSF in order to fulfill the requirements of the program.

Can any CPA firm issue a joint SOC2/HITRUST CSF Certified report?

No. While a CPA firm can perform a SOC2 based on the HITRUST CSF, per the requirements of the HITRUST CSF Assurance Program, only authorized assessors can issue reports that grant HITRUST CSF certification. We currently have a growing list of over 30 assessor firms. Many of these are CPA firms. If the current firm you use for your SOC2 is not on the list, we would encourage you to ask what their plans are related to becoming an authorized HITRUST CSF assessor. Some may already be going through the process.

References:* ***Risk Management Frameworks*, ***CSF Assurance Program Requirements*** *and* ***Risk Analysis Guide***

How is HITRUST and covered entities engaging with the HITRUST 3rd Party Assurance?

HITRUST formed a Business Associate Council in March 2016. The Council was established to ensure healthcare industry business associates and other key vendors are able to influence and directly engage with HITRUST, healthcare organization relating to the HITRUST 3rd Party Assurance program, and other programs impacting business associates.