HITRUST®

HITRUST CSF® Assessor Requirements

Contents

Introduction

Purpose

HITRUST® requires partner organizations and the individuals of partner organizations to meet certain thresholds before receiving authority to perform HITRUST related work, including assessments and certifications. The purpose of this document is to outline the requirements for those professional services firms and individuals seeking approval to provide services to organizations related to the HITRUST CSF.

Qualified Resources

HITRUST defines two classifications of qualified resources, HITRUST CSF Assessors and HITRUST CSF Practitioners.

HITRUST CSF Assessors is a designation reserved for organizations with the core business function of providing security, risk, and consulting services to other organizations, particularly in the healthcare industry.

HITRUST CSF Practitioners is a designation reserved for individuals who have the background, experience, training, and understanding to effectively use the HITRUST CSF. Such individuals either work for a HITRUST CSF Assessor organization, a HITRUST member organization, or a firm/practice that provides HITRUST CSF consulting services.

External References

The following HITRUST documents, located on the HITRUST website under HITRUST CSF Assurance & Related Programs in the "downloads" tab, should be referenced for program background and familiarity with the HITRUST CSF as this document only addresses the process and requirements for organizations providing services for the HITRUST CSF:

- HITRUST CSF Assessment Methodology
- HITRUST CSF Assurance Program Requirements
- CSF and CSF Assurance Program Requirements for Health Information Exchanges

HITRUST CSF Assessors

General

HITRUST CSF Assessors are those professional services firms that have been approved by HITRUST for performing assessment and/or certification services associated with the HITRUST CSF.

Applying to HITRUST

Organizations seeking the HITRUST CSF Assessor designation must provide a letter from an authorized member of management to HITRUST committing the firm to support HITRUST member organizations with qualified resources for any HITRUST CSF related service. The organization must also have documented policies and procedures that it follows to help ensure the integrity and ethics of its employees. HITRUST requires the organization to provide a copy of this documentation for review. Once approved by HITRUST, this documentation must be held and maintained within the

organization's appropriate records department. Organizations seeking the HITRUST CSF Assessor designation must complete and provide to HITRUST the following:

- **HITRUST CSF Assessor application documents (see Appendices A and B):** These documents serve to provide HITRUST with background information on the organization including scope of services offered, years of service in information security and healthcare industry, and the number of individual resources focused in these areas.
- **Documented policies and procedures around how the organization would complete any type of HITRUST CSF-related engagement:** This documentation is to include the organization's policies and procedures for conducting assessments and its quality assurance and review process for ensuring high quality of services and deliverables. The documentation should explain how the assessment will be conducted, who will be reviewing the assessment results, and the deliverables that will be created. HITRUST will use this documentation to gain confidence that assessments will be performed in a thorough manner and the type of documentation it can expect to receive for a completed assessment being submitted to HITRUST for its review.
- **Documented policies and procedures the organization follows to ensure the integrity and ethics of its employees**
- **The names and resumes of the individuals committed to be trained as HITRUST CSF Practitioners:** When additional individuals are sent to training to become HITRUST CSF Practitioners, resumes must also be provided prior to the date of the class to verify they have the requisite experience. HITRUST requires the organization to provide a copy of this documentation, which will be used to support decisions surrounding the competence and integrity of the organization and will keep all documentation fully confidential.

Once approved by HITRUST, this documentation must be held and maintained within the organization's appropriate records department.

Organizations seeking the HITRUST CSF Assessor designation must adhere to the fee structure defined by HITRUST and execute the HITRUST CSF Qualified Assessor Agreement to qualify for providing HITRUST CSF related services.

Upon approval of the application and policies, and execution of the approved HITRUST CSF Assessor Agreement by HITRUST, HITRUST will submit a letter to the organization's authorized member of management serving as the agreement that formalizes the organization's HITRUST CSF Assessor status.

Engagement Team Requirements

At a minimum the following individual(s)[1] from the engagement team performing the assessment and/or certification work must be Certified CSF Practitioners:

- Engagement Executive or the Quality Assurance Review Executive
- Onsite team leader/manager responsible for the field work

[1] *The organization must commit a minimum of 5 individuals to support HITRUST CSF services. If this provision cannot be met due to constraints on the number of client servicing individuals focused on healthcare or information security, the organization shall notify HITRUST to discuss alternatives.*

It is expected that at least a third of the engagement hours would be performed by Certified HITRUST CSF Practitioners to ensure the team has an appropriate understanding of the industry and information security, the HITRUST CSF, and HITRUST CSF assurance methodologies and tools.

Organizations will provide HITRUST with a resume of everyone selected by the organization to be a Certified HITRUST CSF Practitioner to validate education, years of working experience, responsibilities and any relevant certifications. Organizations will attest that the individuals seeking qualification have passed a criminal background check at the time of hire, which shall include at a minimum:

- Education for the highest-awarded degree
- Prior full-time employment
- Criminal records for as far back as the county/state/federal governments have records

When additional individuals are sent for training, the organization will have to attest that they have performed a criminal background check for these individuals as well. See Appendix C for a letter template that can be used during the initial assessor application process and when sending additional people for training.

At a minimum, members of the assessment team will possess the technical competence to match the classification of the HITRUST member organization to which services are being provided. For example, if a hospital system was being assessed, at a minimum the team lead, and any functional leaders, would be expected to have provider healthcare knowledge and experience.

Peer Review

To ensure adherence to both HITRUST and the organization's policies and procedures, HITRUST reserves the right to perform a review of the HITRUST CSF Assessor organization. Based on the organization and its past performance of HITRUST CSF related work, the peer review would be one or a combination of the following approaches:

- HITRUST or an organization selected by HITRUST would re-perform the assessment/review to validate the results documented by the HITRUST CSF Assessor.
- HITRUST or an organization selected by HITRUST would select an engagement that was performed during the past twelve (12) months and perform a more rigorous review of the work papers, identify how well the assessment/review activities were documented, and identify how well the activities complied with the HITRUST CSF Assessor's and HITRUST policies and procedures.

CSF Practitioners

General

HITRUST CSF Practitioners (individuals) are either

- members of a HITRUST assessor organization that have obtained this status through the HITRUST training class to assist organizations with certifications
- are independent consultants who have completed the HITRUST training class and assist organizations with self-assessments or implementing the CSF in their environment

Individuals do not have to be part of an assessor firm to be a practitioner. Anyone who completes the class, passes the exam, and meets the other requirements is a practitioner.

Prerequisites

Individuals seeking the Certified HITRUST CSF Practitioner designation must have, at a minimum, two (2) years of information security expertise (e.g., security and privacy policy development/implementation, risk management, risk assessment/analysis/mitigation.

As noted above a resume for each individual working for an assessor organization and seeking status as a Certified HITRUST CSF Practitioner must be provided to HITRUST to validate the individual's education, years of working experience, individual work-related responsibilities, and any relevant certifications achieved where required. Also, as noted above, the assessor organization must attest to performing a background check of the individual.

Training

Individuals seeking the Certified HITRUST CSF Practitioner designation that have been approved by HITRUST must initially attend and complete the training offered by HITRUST, (including refresher courses), and again every third year to ensure current and consistent knowledge of the HITRUST CSF and related tools and methodologies. At the end of training, the individual must successfully pass the final examination associated with the course to demonstrate competence.

Continued Education

Individuals who have attained the CSF Practitioner designation must meet the following continued education requirements to maintain the designation:

- Obtain a minimum of 120 CPEs every three (3) years
- Complete the CBT HITRUST Refresher Course at the end of the first and second year following the completion of onsite training
- Maintain employment in the field of information security

Audit of Continued Education

HITRUST reserves the right to request further evidence of attendance at any training course that a Certified HITRUST CSF Practitioner has attended in conjunction with the 120 CPE three-year requirement. On an annual basis HITRUST will randomly select certain Certified HITRUST CSF Practitioners and ask them to submit proof of such training. Where the Practitioner possesses complimentary certifications (e.g., CISSP, CISM, CISA) providing HITRUST his/her certification number will suffice as that allows HITRUST to verify compliance.

Appendix A: HITRUST CSF Assessor Application Letter

- *HITRUST CSF Assessor Application Letter Template*

Appendix B: HITRUST CSF Assessor Application

- *HITRUST CSF Assessor Application Template*

Appendix C: HITRUST CSF Assessor Background Check

- *HITRUST CSF Assessor Background Check Letter Template*

If you are interested in becoming a an approved HITRUST CSF Certified Assessor, please contact us at assessor@hitrustalliance.net.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net