

HITRUST

CSF Assessor

Requirements

Version 1.1

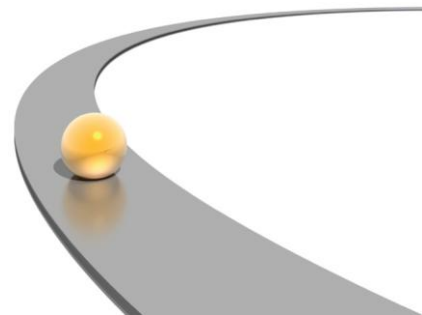
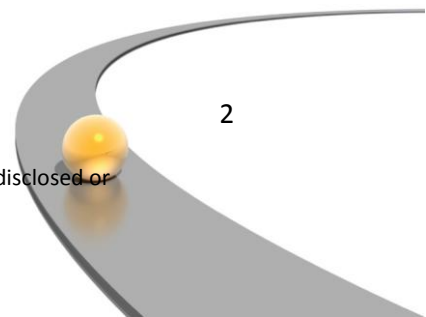


Table of Contents

1	Introduction	3
1.1	Purpose	3
1.2	Qualified Resources	3
1.3	External References	3
2	CSF Assessors	4
2.1	General.....	4
2.2	Applying to HITRUST	4
2.3	Resource Requirements.....	5
2.4	Peer Review.....	5
3	CSF Practitioners	7
3.1	General.....	7
3.2	Prerequisites	7
3.3	Training	7
3.4	Continued Education.....	7
	Appendix A – CSF Assessor Application Letter.....	8
	Appendix B – CSF Assessor Application	9
	Appendix C – CSF Assessor Background Check.....	10
	Appendix D – CSF Assessor Application Process.....	11



1 Introduction

1.1 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 Common Security Framework (CSF). All qualified resources, including both organizations and individuals, must obtain a license to the CSF by registering on HITRUST Central.

1.2 Qualified Resources

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

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.

CSF Practitioners is a designation reserved for individuals who, as part of a CSF Assessor organization or a HITRUST member organization (e.g., a hospital), have the background, experience, training, and understanding to effectively use the CSF.

1.3 External References

The following HITRUST documents, located on HITRUST Central in the “downloads” section, should be referenced for program background and familiarity with the CSF as this document only addresses the process and requirements for organizations providing services for the CSF:

- HITRUST CSF Executive Summary and Introduction
- HITRUST CSF Implementation and Assessment Methodology
- HITRUST CSF Assurance Program Requirements

2 CSF Assessors

2.1 General

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

2.2 Applying to HITRUST

Organizations seeking the 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 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 CSF Assessor designation must complete and provide to HITRUST the following:

- CSF Assessor application documents (attached) – 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 CSF-related engagement – This documentation is to include the organization's own quality assurance and review process for ensuring high quality of services and deliverables. The documentation should explain at a minimum 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 have been performed in a thorough manner.
- 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 – As new individuals are sent to training to become HITRUST CSF Practitioners, resumes must also be provided prior to the date of the class.

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 CSF Assessor designation must adhere to the fee-structure defined by HITRUST and execute the Common Security Framework Qualified Assessor Agreement to qualify for providing CSF related services to HITRUST member organizations.

Upon approval of the application and policies, and execution of the 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 CSF Assessor distinction.

2.3 Resource Requirements

The individual(s)¹ from the organization leading the team who will perform the assessment and/or certification work must be a CSF Practitioner, meeting the requirements in addition to attending and passing the applicable training outlined in section 3 of this document. It is recommended that a majority of the engagement team be CSF Practitioners to ensure an appropriate understanding of healthcare and information security, and the methodologies, tools and CSF.

Organizations will provide HITRUST with a resume of each individual selected by the organization to be a 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.

See Appendix C for a letter template.

At a minimum, 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, the assessment team requires healthcare knowledge for providers as opposed to payers.

2.4 Peer Review

To ensure adherence to both HITRUST's and the organization's policies and procedures, HITRUST will periodically, at least annually, perform an onsite peer review of the CSF Assessor organization. Based on the organization and its past performance of CSF related work, the peer review will be one or a combination of the following approaches:

- HITRUST will re-perform the assessment/review of a member organization to validate the results documented by the CSF Assessor.

¹ The organization must commit a minimum of 5 individuals to support HITRUST 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.

- HITRUST will 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 CSF Assessor's and HITRUST's policies and procedures.

3 CSF Practitioners

3.1 General

CSF Practitioners are those individuals working as part of a CSF Assessor organization or HITRUST member organization who provide or perform CSF related services or activities.

3.2 Prerequisites

Individual seeking the CSF Practitioner designation must meet the following requirements:

- Have, at a minimum, two (2) years of expertise in the healthcare industry (e.g., payer, provider, clearinghouse, federal).
- Have, at a minimum, two (2) years of information security expertise (e.g., threats, vulnerabilities, and impacts including techniques for their reduction and control).

A resume for each individual 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.

3.3 Training

Individuals seeking the CSF Practitioner designation that have been approved by HITRUST as mentioned above must initially attend and complete the training offered by HITRUST, and again every third (3rd) year to ensure current and consistent knowledge of the CSF and related tools and methodologies. At the end of training, the individual must successfully pass the final examination associated with the course to prove competence.

3.4 Continued Education

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

- Active involvement with the HITRUST community.
- Participation in at least one (1) HITRUST or other healthcare or security committee/working group annually.
- Maintain and submit proof to HITRUST a minimum of 120 CPEs every three (3) years.
- Attend a HITRUST training update course annually and pass the associated examination.
- Attend the complete training offered by HITRUST every third (3rd) year and pass the associated examination.
- Maintain employment in the field of information security.

Appendix A – CSF Assessor Application Letter

CSF Assessor Application Letter Template.



Application_Letter_T
EMPLATE.doc

Appendix B – CSF Assessor Application

CSF Assessor Application Template.



Application.doc

Appendix C – CSF Assessor Background Check

CSF Assessor Background Check Letter Template.



Background_Check_
TEMPLATE.doc

Appendix D – CSF Assessor Application Process

CSF Assessor Application Process.



CSF_Assessor_Application_Process.pdf