



## **HITRUST External Assessor Requirements**

---

# Contents

- Introduction ..... 3**
  - Purpose ..... 3**
  - Qualified Resources ..... 3**
  - External References ..... 3**
- HITRUST External Assessors ..... 3**
  - General ..... 3**
  - Applying to HITRUST ..... 3**
  - Engagement Team Requirements ..... 4**
  - Segregation of Assessor Duties ..... 4**
  - Peer Review ..... 5**
- Certified CSF Practitioners and Certified HITRUST Quality Professionals ..... 5**
  - General ..... 5**
  - Prerequisites ..... 5**
  - Training ..... 6**
  - Continued Education ..... 6**
  - Audit of Continued Education ..... 6**
- Appendix A: HITRUST External Assessor Application Letter ..... 7**
- Appendix B: HITRUST External Assessor Application ..... 7**
- Appendix C: HITRUST External Assessor Background Check ..... 7**

## Introduction

### Purpose

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

### Qualified Resources

HITRUST defines three classifications of qualified resources:

- **Authorized HITRUST External Assessor** is a designation reserved for professional services firms or business units with the core business function of providing security, risk, and consulting services to other organizations.
- **Certified CSF Practitioner (CCSFP)** is a designation reserved for individuals who have completed the CCSFP training course, passed the certification exam, and have met the required background and experience requirements necessary to effectively use the HITRUST CSF. Such individuals typically work for a HITRUST External Assessor organization, a HITRUST CSF user organization, or a firm/practice that provides HITRUST CSF consulting services.
- **Certified HITRUST Quality Professional (CHQP)** is a designation reserved for Certified CSF Practitioners who act in a quality assurance role on HITRUST assessment engagements, have completed the CHQP training course, and have passed the CHQP certification exam. Such individuals typically work for a HITRUST External Assessor organization.

### External References

The following HITRUST documents, located on the HITRUST website under *HITRUST Assurance Program* in the “relevant resources” tab, should be referenced for program background and familiarity with the HITRUST CSF:

- *HITRUST Assurance Program Requirements*

## HITRUST External Assessors

### General

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

### Applying to HITRUST

Organizations seeking the HITRUST External Assessor designation must provide a letter from an authorized member of management committing to support HITRUST member organizations with qualified resources for any HITRUST CSF-related service. The organization must observe documented policies and procedures 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 External Assessor designation must complete and provide to HITRUST the following:

- **HITRUST External Assessor application documents (see Appendices A and B and C)** These documents serve to provide HITRUST with background information on the organization including scope of services offered, years of service in the information security industry, and the number of individual resources focused on security and privacy services.

- **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 CCSFPs and CHQPs** Organizations must provide HITRUST with the résumé –if possible, of everyone selected by the organization to be a CCSFP and and CHQP. These will be used by HITRUST to validate education, years of working experience, responsibilities, and any relevant certifications. HITRUST will also use this documentation to support decisions surrounding the competence and integrity of the organization. HITRUST will keep all documentation fully confidential. Please list which individuals are committed to be trained as Certified HITRUST Quality Professionals. The organization must commit a minimum of five individuals to be certified as CCSFPs and two individuals to be certified as CHQPs (which can be included amongst the 5 CCSFPs). If these provisions cannot be met due to constraints on the number of client servicing individuals focused on HITRUST assessments or information security, the organization shall notify HITRUST to discuss alternatives.

Organizations seeking the HITRUST External Assessor designation must also adhere to the fee structure defined by HITRUST, and they must execute the HITRUST External Qualified Assessor Agreement. Upon approval of the application and associated documentation, and upon execution of the approved HITRUST External Assessor Agreement by HITRUST, HITRUST will send a letter to the organization's authorized member of management serving as the agreement that formalizes the organization's HITRUST External Assessor status.

### Engagement Team Requirements

HITRUST requires that the following engagement team members hold the CCSFP designation:

- On-site team lead / manager responsible for assessment fieldwork
- Engagement executive
- Engagement's quality assurance reviewer

Assessment teams submitting validated assessments to HITRUST are required to have at least one CHQP act in the role of quality assurance reviewer. To ensure the team has an appropriate understanding of the HITRUST CSF and HITRUST CSF assurance methodologies and tools, HITRUST also requires that at least 50% of all validated assessment engagement hours be performed by CCSFPs.

### Segregation of Assessor Duties

In order to ensure independence and objectivity of the authorized External Assessor firm, HITRUST-relevant consulting services must be segregated from HITRUST validated assessment services. In practice, this means:

- Any assessor firm professionals performing HITRUST-relevant consulting services for an organization (e.g., facilitated self-assessments, readiness assessments, remediation efforts) within the prior 12 months may not work on the validated assessment for that organization. A separate team (including a separate engagement executive / partner) should be brought in for the validated assessment effort.
- If any assessor firm personnel operate a control for an assessed entity within the prior 12 months, that assessor firm cannot be engaged by that assessed entity to perform the validated assessment.
- If any assessor firm provides example policies, procedures, checklists, etc. which are adopted by an assessed entity, the assessor firm professionals who prepared those documents cannot participate in the validated assessment effort.

Additionally, HITRUST stipulates that the individual acting as a validated assessment's CHQP/quality reviewer may not perform any other duty on that assessment, such as client-facing engagement executive, field work lead, etc. This requirement helps ensure that the assessor's pre-submission quality review is performed with objectivity.

### 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 External Assessor organization. Based on the organization and its past performance of HITRUST CSF-related work, this review could be one or a combination of the following approaches:

- HITRUST or an organization selected by HITRUST will re-perform one or more assessments/reviews to validate the results documented by the HITRUST External Assessor.
- HITRUST or an organization selected by HITRUST will select an engagement performed during the past twelve (12) months and perform a more rigorous review of the work papers, identify how well the assessment/review activities are documented, and identify how well the activities comply with the HITRUST External Assessor's and HITRUST Assurance Program policies and procedures.

## Certified CSF Practitioners and Certified HITRUST Quality Professionals

### General

Certified CSF Practitioners (CCSFPs) and Certified HITRUST Quality Professionals (CHQPs) are typically:

- HITRUST assessor organization employees who completed the HITRUST CSF training class(es) and are assisting organizations with becoming HITRUST certified.
- Organization employees who have completed the HITRUST CSF training class and are actively working towards implementing the CSF framework in their organizations.
- Independent consultants who have completed the HITRUST CSF training class and are assisting organizations with self-assessments or implementing the CSF framework in their environment.

Individuals do not have to be employed by an assessor firm or a HITRUST CSF user organization to be a CCSFP or a CHQP. Anyone who completes the class, passes the exam, and meets the other requirements can become a CCSFP/CHQP.

### Prerequisites

Individuals seeking the CCSFP designation must have, at a minimum, two (2) years of information security and/ or technical assessment expertise (e.g., security and privacy policy development/implementation, IT audit, risk management, risk assessment/analysis/mitigation).

As noted above, a résumé for each individual working for an assessor organization and seeking status as a CCSFP must be provided to HITRUST to validate the individual's education, years of work experience, individual work-related responsibilities, and any relevant certifications. As noted above, the assessor organization must attest to performing a background check of the individual. Also, as noted previously, in order to obtain the CHQP certification, the individual must be a CCSFP.

## Training

The CCSFP designation requires that candidates attend and complete in-person/on-site training class offered by HITRUST, annual web-based refresher courses, and an in-person training offered by HITRUST every third year to ensure current and consistent knowledge of the HITRUST CSF and related tools and methodologies. Individuals seeking the CHQP designation must complete a web-based training course at time of initial application. The CHQP designation is valid for two years, and re-certification requires completion of a web-based refresher course and exam. At the end of these trainings, the individual must successfully pass an examination associated with the course to demonstrate competence.

## Continued Education

Individuals who have attained the CCSFP or CHQP designation must meet the following continued education requirements to maintain the designation:

- Obtain a minimum of 120 CPEs every three years
- Completion of required training course(s) annually as described in the “Training” section above
- Maintain employment in the field of information security

## Audit of Continued Education

HITRUST reserves the right to request further evidence of attendance for any training course that a CCSFP or CHQP has submitted in conjunction with the 120 CPE three-year requirement. On an annual basis, HITRUST will randomly select certification holders and ask them to submit proof of training. Certification numbers of complementary designations (CISSP, CISM, CISA, etc.) will suffice as verification.

If you are interested in becoming an approved HITRUST External Certified Assessor, please contact us at [csfassessor@hitrustalliance.net](mailto:csfassessor@hitrustalliance.net).

## **Appendix A: HITRUST External Assessor Application Letter**

*Organizations seeking the HITRUST External Assessor designation must provide the **HITRUST External Assessor Application Letter** on company letterhead. Please send this letter to [csfassessor@hitrustalliance.net](mailto:csfassessor@hitrustalliance.net).*

## **Appendix B: HITRUST External Assessor Application**

*Organizations seeking the HITRUST External Assessor designation must complete and submit the **HITRUST External Assessor Application form** to HITRUST for review and approval. Please send the completed form to [csfassessor@hitrustalliance.net](mailto:csfassessor@hitrustalliance.net).*

## **Appendix C: HITRUST External Assessor Background Check**

*Organizations seeking the HITRUST External Assessor designation must provide the **HITRUST External Assessor Background Check Attestation** on company letterhead. Please send this document to [csfassessor@hitrustalliance.net](mailto:csfassessor@hitrustalliance.net).*

**HITRUST<sup>®</sup>**

855.HITRUST  
(855.448.7878)

[www.HITRUSTAlliance.net](http://www.HITRUSTAlliance.net)