

## CSF Assessment Methodology

---

# Contents

- Introduction. . . . . 4**
  - Assessment Process Flow . . . . . 4**
- Project Startup (Step 1). . . . . 6**
  - Identify Project Coordinator. . . . . 6**
  - Define Project Management Organization Structure and Standards. . . . . 6**
  - Assessment Kickoff . . . . . 7**
- Assessment Scoping . . . . . 7**
  - Purpose. . . . . 7**
  - Define Organizational Scope (Step 2) . . . . . 7**
    - Identifying the Business Units. . . . . 7**
    - Organizational Factors. . . . . 8**
    - Regulatory Factors. . . . . 8**
    - Document Organizational and Regulatory Factors . . . . . 9**
  - Define System Scope (Step 3) . . . . . 9**
    - Information Systems Identification. . . . . 9**
    - System Grouping . . . . . 10**
    - Systems that are Centrally Located and Managed . . . . . 11**
    - Vendor Applications . . . . . 11**
    - Document System Factors . . . . . 12**
  - Provide Document Request Listing . . . . . 12**
  - Schedule Stakeholder Interviews. . . . . 12**
- Assessment Approach . . . . . 13**
  - Objective . . . . . 13**
  - Implementation Requirement Levels . . . . . 13**
  - MyCSF. . . . . 13**

# Contents

- Examine Documentation and Practices (Step 4) ..... 14
- Conduct Interviews (Step 5)..... 15
- Perform/Review Technical Testing (Step 6)..... 15
  - Sampling ..... 16
  - Sample Size ..... 16
  - Selecting a Sample ..... 17
  - Control Exceptions or Deviations ..... 18
- Document Findings..... 18
  - Alternate Control Identification and Selection (Step 7) ..... 18
  - Identifying and Selecting Alternate Controls ..... 19
  - Alternate Control Requests..... 19
- Reporting & Remediation ..... 19
  - Reporting (Step 8) ..... 19
    - Develop Remediation Guidance ..... 19
    - Submit Information to HITRUST ..... 19
    - Socializing the Report ..... 20
    - Management’s Response..... 20
    - Sharing the Report ..... 20
  - Remediation (Step 9) ..... 20
  - Risk Acceptance ..... 21

## Introduction

HITRUST collaborated with business, technology, and information security leaders to establish the first ever framework, HITRUST CSF (CSF), to be used by any and all organizations that create, access, store, or exchange sensitive information. HITRUST is also driving adoption and widespread confidence in the CSF and sound risk mitigation practices through the HITRUST community that provides awareness, education, advocacy, support, knowledge sharing and additional leadership and outreach activities.

The HITRUST CSF leverages and enhances existing standards and regulations to provide organizations of any size with prescriptive implementation requirements. By engaging HITRUST and implementing the CSF, certified organizations will have a common privacy and security baseline and mechanism for communicating validated security and privacy controls to different constituents, including regulators, auditors, business partners, and customers.

This document communicates the process to prepare for and perform an assessment of an organization's existing control infrastructure against the HITRUST CSF, provide increased assurance, and meet the following objectives:

- Identify critical information systems storing, processing, or transmitting sensitive information
- Identify, classify, and manage vulnerabilities based on their relative risk to the company
- Provide the organization an awareness of its state of compliance with the CSF
- Establish and prioritize solutions that address root-cause issues to mitigate system vulnerabilities.

### Assessment Process Flow

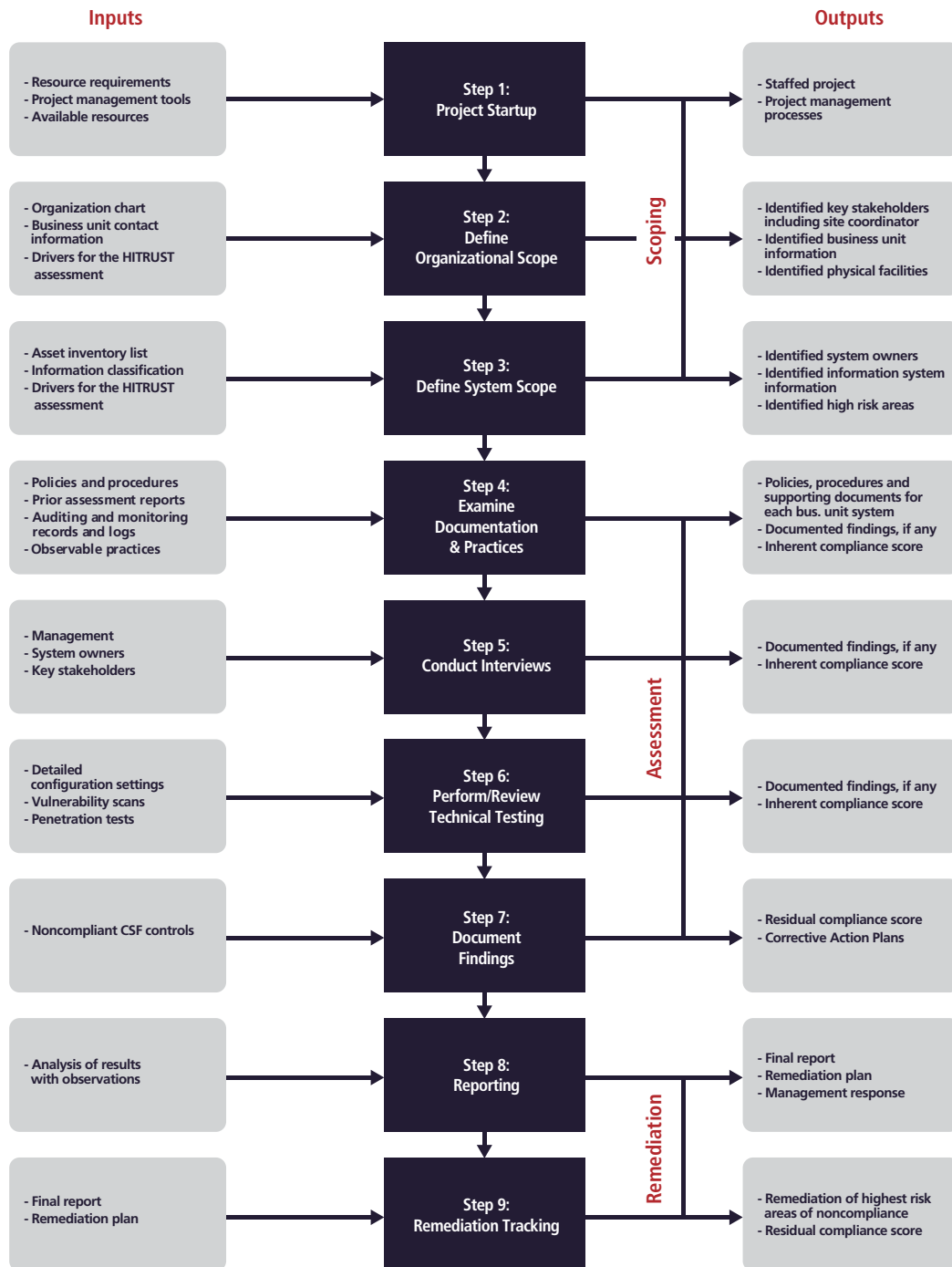
At a high level, the process will follow the steps below:

1. Identify the project coordinator and the supporting review team personnel at the organization being assessed and project management techniques to be used.
2. Define the scope of the assessment in terms of business units and identify appropriate stakeholders from each business unit, including a coordinator.
3. Define the scope of the assessment for each business unit in terms of systems, including those with higher risk profiles (e.g., store, process or transmit sensitive information).
4. Gather and examine the necessary information (e.g., policies, procedures, records, logs, vulnerability assessment reports, risk assessment reports) and examine configuration settings, physical surroundings, processes, and other observable information protection practices.
5. Conduct interviews with the business unit stakeholders, where applicable.
6. Perform system tests to validate the implementation of controls, as applicable.
7. Select and document any Alternate Controls for any noncompliant controls and/or opportunities to enhance existing controls.

- 8. Develop the assessment report with all noncompliant controls and document any recommended remediation tasks in formal corrective action plans (CAPs).
- 9. Finalize report and begin tracking any remediation activities.

A visualization of the process flow can be found on the following page. Subsequent sections of this document describe this process in greater detail.

## HITRUST CSF Assessment Activities



## Project Startup (Step 1)

The purpose of the start-up process is to provide a framework for establishing the organizational and logistical requirements to accurately determine the scope and the structure of the assessment.

### Identify Project Coordinator

The project coordinator is critical to the success of the assessment for communicating expectations to other organizational personnel, gathering documentation, coordinating interviews, and providing insight throughout the assessment. This person should have sufficient authority within the organization to gain access to other executives, influence participation in the assessment, and generally represent the commitment of senior management to the assessment. The organization should formally designate a project coordinator approximately 6 weeks before the fieldwork commences.

### Define Project Management Organization Structure and Standards

The project coordinator should work with the organizational stakeholders to define and agree upon the management structure for the assessment and any standards, procedures, or tools needed to support the project management process. The assessment project management tools will typically include the following documents and sections:

- Project Plan
- Interview Tracking
- Documentation Request Tracking
- Stakeholder/Contact Tracking
- Meeting Minutes
- Weekly Project Status

Any issues or risks that arise during the course of the project can either be maintained within the weekly project status document or in a separate issue/risk tracking log. In either case, the project coordinator should always track and monitor risks as they relate to the project. At a minimum, the following items should be tracked:

- Description of issue/risk
- Action required to resolve the issue/risk
- Priority of the issue/risk
- Date the issue/risk is identified
- Date the issue/risk is resolved
- Individual(s) responsible for resolution

Depending on the complexity and scope of the assessment, additional project management tools and templates may need to be developed.

## Assessment Kickoff

Before beginning the scoping and assessment process, the assessment team should conduct an official kickoff meeting. The meeting should occur 3-4 weeks prior to the assessment fieldwork and should include the assessment team, the external assessor (if applicable), the project coordinator, and any identified key organizational stakeholders. The meeting, at a minimum, should cover the following:

- Assessment team contact information (including the external assessor team, if applicable based on the assessment type)
- Why the organization is performing a HITRUST assessment and its importance to achieving the organization's goals
- Overview of the assessment process and timeline
- High-level scope in terms of covered facilities, systems, system layers (e.g., servers, databases, firewalls), and business units
- Expectations of the organization in terms of meeting participation, evidence collection, responsiveness, etc.
- Status meetings and status communications

## Assessment Scoping

### Purpose

The assessment scoping process is the method for determining which systems, system layers, business units, and facilities will be the focus of the assessment. Using MyCSF, scoping of the HITRUST CSF requirement statements is also determined in this phase.

### Define Organizational Scope (Step 2)

This section focuses on the key task of identifying the business units and key contacts within the organization and documenting the organizational factors that define the level of control for the CSF assessment. Once complete, the assessment team can work with the identified coordinator and contacts within each business unit to determine the system scope and ensure a comprehensive review is performed.

### Identifying the Business Units

A critical step in the assessment scoping process is to break up the organization into auditable business units to ensure the successful management of the assessment. An auditable business unit is defined as units or departments within the organization that can operate distinctly from one another. However, depending on the size and complexity of the organization, they may also represent geographical regions or associations with other (external) groups. Both distinctions are acceptable for the purposes of the CSF assessment and CSF Validation/Certification.

The project coordinator should work with the assessment team and management to define the organization in terms of auditable business units. Once complete, the key contacts within each business unit should be identified along with a business unit coordinator to assist with the performance of the assessment tasks. The key contacts within each business unit include the department head(s), directors, managers, system owners, information security personnel, risk/compliance personnel, human resource personnel, and general users. This list is not exhaustive and may need to be expanded depending on the organization.

### Identifying the Physical Facilities

Another critical step in the assessment scoping process is to define the organization in terms of its physical footprint and determine which sites are relevant to the HITRUST CSF assessment. Facilities to consider include administrative offices, satellite locations, clinics, data centers, co-locations, manufacturing sites, etc. Once complete, the key contacts within each facility should be identified to assist with the performance of the assessment tasks necessary related to that facility. The key contacts within each facility could include the physical security personnel, environmental protection system leads, equipment maintenance personnel, and the office/site manager. In determining whether a facility should be considered in-scope for the assessment, consider questions such as:

- Does the facility house any users of the system(s) being included in the assessment scope?
- Is sensitive information stored on, accessed by, or transmitted from devices housed in the facility?
- Could unauthorized physical access to the facility reasonably lead to a breach of sensitive information?
- Would the readers of your organization's HITRUST report reasonably expect the facility to be included in the assessment scope?

### Regulatory Factors

The CSF also defines a number of regulatory factors based on the compliance requirements applicable to an organization:

- Subject to FISMA Compliance
- Subject to FTC Red Flags Rule Compliance
- Subject to Joint Commission Accreditation
- Subject to PCI Compliance
- Subject to State of Massachusetts Data Protection Act
- Subject to the CMS Minimum Security Requirements (High)
- Subject to the State of Nevada Security of Personal Information Requirements
- Subject to Texas Health and Safety Code
- Subject to MARS-E Requirements
- Subject to IRS Pub 1075 Compliance
- Subject to HITRUST De-ID Framework Requirements



- Subject to CA Civil Code § 1798.81.5
- Subject to EHNAC Accreditation
- Subject to Banking Requirements
- Subject to FedRAMP Certification Requirements
- Subject to 21 CFR Part II
- Subject to 23 NYCRR 500
- Subject to CRR V2016
- Subject to the EU GDPR
- Subject to HIPAA
- Subject the Personal Data Protection Act
- Subject to Supplemental Requirements

### **Document Organizational and Regulatory Factors**

The organizational, regulatory, and system factors (see Document System Factors) are used to determine the level of implementation requirements for a selection of controls/control requirements within the CSF.

Once the organization has identified the auditable business units within scope, the above information should be gathered for the organization as a whole and for each business unit and documented in the MyCSF tool. Once complete, the relevant level(s) of control will be provided with the associated assessment requirements statements to determine compliance with the CSF.

### **Define System Scope (Step 3)**

This section focuses on scoping the information systems that will be the primary focus of the CSF assessment. Once complete, the organization will be able to identify areas of higher risk and ensure a comprehensive review. The following steps should be taken in order to identify the information systems within scope of the CSF assessment.

### **Information Systems Identification**

This section focuses on scoping the information systems that will be the primary focus of the CSF assessment. Once complete, the organization will be able to identify areas of higher risk and ensure a comprehensive review. The systems to include in the scope of the HITRUST assessment should be determined by the drivers for performing the assessment. Organizations seeking to demonstrate holistic compliance with a particular set of regulatory factors (e.g., GLBA, HIPAA) should use a “follow the sensitive data” approach to system scoping. Organizations needing

to satisfy customer requirements through achievement of a HITRUST certification would select only those systems used in the delivery of services to customers. Organizations seeking to validate controls within a business unit or department would likely need to scope in all systems used by that business unit or department in the achievement of departmental objectives. The assessment team should leverage an up-to-date system inventory listing and work with the business unit coordinator and key security contacts within the organization to identify systems for the CSF assessment. The key security contacts can help focus and streamline analysis and information gathering tasks by clearly identifying systems and the related system elements upfront in the assessment process.

While a certain degree of flexibility is allowed in scoping a HITRUST assessment, the following considerations should be observed:

- While the controls of the CSF are designed to apply to all information systems irrelevant of classification or function, systems used to store, process, access, protect, or transmit sensitive information should be the focus of the HITRUST assessment.
- When scoping a particular application or product, all system / technology layers should be included. For example, when assessing a Web application, layers such as the server, Web application, underlying database, etc. should be included. As another example, the elements of an imaging system used in healthcare will include the imaging application, the underlying operating system, interfaces with the application, the underlying database, and the physical servers. Infrastructure components, such as routers and firewalls, that are connected to or facilitate the transmission of sensitive information to/from these systems should also be included.
- Terminals / workstations / mobile devices / endpoints used to access the system(s) or environment(s) deemed in-scope for the HITRUST assessment must, by proxy, be evaluated during the HITRUST CSF assessment, as certain CSF domains (mobile devices, portable media, and configuration management) address risks specific to such devices.
- The facilities housing all in-scope systems should be included in the scope of the HITRUST effort. For example, if servers reside in a co-location environment, physical and environmental controls operating in that co-location are important to the overall security of the in-scope systems.

### **System Grouping**

When assessing systems, it is appropriate to aggregate information into one observation if it meets all of the following conditions:

- It is under the same direct management control
- It has the same function or mission objective
- It has essentially the same operating characteristics and security needs (confidentiality and criticality)
- It resides in the same general operating environment

The purpose of this aggregation is to logically group systems so that the assessment is performed, and information reported in a comprehensive yet manageable manner. It is not necessary to complete the assessment for every element. For example, if an application runs on several different servers, and all of the servers run the same operating system, are located in the same server room, and managed by the same group, the analysis can be performed, and findings documented for a representative sample of the servers. Likewise, a business unit with ten routers that are all from the same vendor, identically configured, managed by the same group, and physically protected in the same way could be analyzed and requirement statements answered for a sample of the routers.

**Systems that are Centrally Located and Managed:** The approach for assessing systems that are located and managed at a centralized data center is based on a business unit’s responsibility over that system. A business unit should focus the assessment on those aspects of the system operations that are directly under its control. For example, there are circumstances when a business unit only has responsibility over establishing accounts and access rights within an application, but all other aspects of the system operation are managed by the data center (e.g., operating system, backups, physical security). In this case, the business unit will only address questions in the CSF assessment related to application access controls. The data center will address CSF assessment questions related to the other operational areas. Both can be documented in a single assessment for the system.

**Vendor Applications:** Similar to the systems at a data center, the approach for vendor-managed systems is based on the business unit’s control of the system. The different scenarios for vendor-managed systems at a business unit and the related risk assessment scope are summarized in the table below:

#	Scenario	Assessment Scope
1	The system is located off-site from a business unit and managed by the vendor except for access control to the application	Questions related to application access
2	The system is located on-site at the business unit but completely managed by the vendor (e.g., dial-up access for administration) except for access control to the application	Questions related to physical security and application access
3	The system is located on-site and is managed by the IS personnel at the business unit with some support from the vendor	All questions

### Document System Factors

The CSF defines a number of System Factors that can increase the inherent risk to the system, necessitating a higher level of control. Each system must be assessed to determine the associated level of control based on the following factors:

- Stores, processes, or transmits sensitive information
- Accessible from the Internet
- Accessible by a third party
- Exchanges data with a third party/business partner
- Publicly accessible
- Use of mobile devices
- Number of interfaces to other systems
- Number of users
- Number of transactions per day

The assessment team should work with the identified business unit coordinator(s) and other key stakeholders to identify all relevant information systems and document the necessary information in MyCSF. In addition to the above-mentioned factors, other information to document includes system owner, platform (e.g., Windows, UNIX), and ID. This information should be gathered and documented one to two weeks before the fieldwork occurs.

### Provide Document Request Listing

The document request list is a list of potentially relevant materials, including policies, procedures and standards used to support an organization's processes. The document request list should be distributed to business units in advance of the assessment. This will allow individuals the time to gather the requested documentation and to contribute to a more efficient process while conducting the assessment. For additional information, refer to the illustrative procedures in the MyCSF tool.

### Schedule Stakeholder Interviews

After completing the initial scoping process, relevant stakeholders should be identified to assist in completing the assessment process. Interviews will provide the assessment team with necessary information regarding any organizational and system controls in place and whether additional documentation, interviews or testing is required. During the interviews, the assessment team should document existing processes (i.e., processes as actually implemented by the organization) and inquire about artifacts that could be used to test the process to determine if it is fully implemented and functioning as described.

It is important to schedule meetings in advance with the appropriate resources to ensure accurate information is collected and to maintain the timeliness of the assessment. Refer to the illustrative procedures in MyCSF for additional information. Also, when a system is included in the assessment scope, it is often necessary to review the application layer, database layer, operating system layer and the network layer. Interviews should typically be scheduled for 1- 2 hours, depending on how much material will be covered.

## Assessment Approach

### Objective

The assessment approach is the method for assessing the organization's controls via data gathering techniques, including document reviews, interviews, and system tests.

- **Examine:** Policies, standards, guidelines, procedures, records, and other observable information protection practices to evaluate support of the control specification
- **Interview:** Management, system owners and select organization personnel with relevant job responsibilities to help verify the procedures and controls are followed
- **Test:** System configurations and functions to validate the requirements of the organization's policies and that the CSF controls are implemented and functioning appropriately

These tests are to be performed by a self-assessing entity or authorized HITRUST External Assessor in determining what controls are implemented within the organization and for each system. Once the necessary information is gathered, the assessment team will document any findings and provide the results of the assessment to HITRUST. (Additional information may be found in the HITRUST CSF Assurance Program Requirements document.)

Similar to the process for assessing scope, the approach should be designed to be flexible and adaptive so a comprehensive assessment can take place within the organization and identified business units with minimal impact on operations.

### Implementation Requirement Levels

The CSF follows a risk-based approach by practically applying security resources commensurate with level of risk and applicable regulations or standards. HITRUST addresses risk by defining levels of implementation requirements, which increase in restrictiveness for each security control. Up to three (3) levels of requirements are defined based on relevant organizational and/or system risk factors. Level 1 provides the baseline control requirements as determined by the industry. Each additional level encompasses the level(s) before it and includes additional requirements commensurate with the increase in risk.

### MyCSF

The MyCSF web-based tool was designed to assist assessing organizations and External assessors in streamlining the assessment approach and identifying applicable CSF controls and implementation requirements. This fully integrated, optimized, and user-friendly tool marries the content and methodologies of the HITRUST CSF and CSF Assurance

program with the technology and capabilities of a Governance Risk and Compliance (GRC) tool. The tool provides assessing organizations and External assessors with a secure, web-based solution for accessing the CSF, performing assessments, and reporting and tracking compliance.

By utilizing the capabilities of a GRC-type platform, MyCSF provides organizations and External assessors with a sophisticated and user-friendly tool in which to scope and execute an assessment. The tool increases the efficiency with which External assessors and organizations can assess against the CSF by utilizing advanced workflows, custom criteria, automated data collection and notifications, and enhanced navigation and search tools. The tool also provides a user-friendly interface with the availability of dashboards and reports and acts as a central repository for managing documents, corrective action plans, test plans, and system scoping.

MyCSF uses a risk-based approach based on organizational, regulatory and system profile information to create a comprehensive and customized set of requirements statements from a standard set of controls. Assessments can be submitted directly to HITRUST for review, scoring and reporting. Assessment types include the following:

- **CSF Security Assessment:** Measures an organization against a streamlined set of requirements from the controls required for CSF Certification, which are identified and selected based upon risk.
- **CSF Security & Privacy Assessment:** Measures an organization against a streamlined set of requirements from the controls required for CSF Certification, which are identified and selected based upon risk, plus all privacy controls
- **CSF Comprehensive Security Assessment:** Measures an organization against a streamlined set of requirements from all 135 controls of the CSF.
- **CSF Comprehensive Security & Privacy Assessment:** Measures an organization against a streamlined set of requirements from all 135 controls of the CSF plus all privacy controls

#### Examine Documentation and Practices (Step 4)

The assessment team can evaluate compliance for all controls by examining information retained by the organization. For a listing of example documents that can be examined during the assessment, please refer to the Examine section of the control assessment guidance in the HITRUST CSF and/or the Illustrative Procedures in MyCSF. At a high-level, examine the documents to validate compliance with the associated requirements within the CSF. At a more granular level, examine documents to identify specific practices for more detailed tests and evaluation.

In addition to gathering and reviewing documentation, examination must include checking, inspecting, reviewing, observing, studying, or analyzing one or more information security practices to facilitate an understanding, achieve clarification, or obtain evidence, which can be used to support the determination of control effectiveness. Examples include observation of processes and procedures, physical and environmental security (camera placement, locked doors, entry controls, emergency power cut-off switches, etc.), and other observable information security practices.

### Conduct Interviews (Step 5)

The previously scheduled meetings with the various stakeholders are conducted to gain an overall understanding of how the organizational and system controls of the CSF are followed. Review the “interview section” of the control assessment guidance in the HITRUST CSF and/or the Illustrative Procedures in MyCSF to identify these stakeholders and what questions should be considered when validating controls.

Before conducting the interviews, the interviewer should take the following steps to understand what questions should be asked during the interview:

- Obtain and review any documentation relevant to the subject area. For instance, if you will be asking about a server’s security policies, ensure that you have reviewed the overall policy regarding system security.
- Based on the interviewee’s role and responsibilities, identify, and ask all related questions.
- Conduct the interviews and document the results in the form of meeting minutes or another suitable tool.

### Perform/Review Technical Testing (Step 6)

Technical testing helps reveal security flaws or weaknesses in information systems and includes but is not limited to configuration setting validation, vulnerability assessment, and penetration testing.

Validation of configuration settings for select system controls provides evidence regarding the implemented security policies and procedures. Configuration settings for high risk applications may include the following:

- Audit settings
- Patch levels
- Password settings
- Account lockout
- Anti-virus data file (DAT) levels
- User listings

Validation of configuration settings helps an assessment team determine if policy requirements have been met, especially with controls related to configuration, change and exception management.

Vulnerability assessments help identify, quantify, and prioritize weaknesses in an information system that may be exploitable by one or more threats. Assessment teams may conduct vulnerability assessments on information systems or review the results of recent vulnerability assessments to help evaluate CSF controls related to, for example, patching and exception management processes. Penetration tests can be used to help an assessment team validate

vulnerabilities identified during a vulnerability assessment as well as help identify additional vulnerabilities within the organization's environment.

Complete the following high-level steps when performing technical testing:

- Obtain the necessary tools, approvals and permissions to perform the system tests.
- Conduct the tests and formally document the results.

Assessment teams should review any internal or external (third party) vulnerability or penetration test documentation that is within the scope of the assessment, especially if the assessment team does not conduct its own.

### **Sampling**

For both CSF Validated and CSF Certified assessments, the assessment team may choose to use a sampling approach when selecting system components to determine the existence of controls. The sample must meet both of the following criteria:

- The sample should be representative of every component of the in-scope systems, applications, databases, networking devices and connected support systems included in the sample population (group).
- The sample should be large enough to allow the assessment team to draw conclusions about the application of controls across the full sample population.

Although not intended to be an authoritative source on sampling, what follows is general guidance that assessment teams should consider when sampling. Where a External Assessor organization has its own internal guidance on sample sizes, they may follow that guidance in lieu of what is described here; however, HITRUST would expect it to be similar to the methods described in this document and this document's sample size requirements should be treated as minimums.

As discussed earlier, items such as systems or auditable business units that are subject to the same controls can be grouped and tested as one sample population, which can be more efficient than testing all items in the population. This is often the case where IT general controls are being tested and common IT processes like change management or password administration support multiple systems.

### **Sample Size**

Once the population to be tested has been identified, the first step is to calculate an appropriate sample size. The table below is based upon the assumption that the controls are operating effectively, and the assessment team does not expect any exceptions.



Nature of Control and Frequency of Performance	Minimum Number of Items to Test
Manual control, performed daily or many times a day, population > 250	25
Manual control, performed weekly	5
Manual control, performed monthly	2
Manual control, performed quarterly	2
IT General Controls (ITGCs)	Same as guidance for manual controls above
Application Control	Can perform a test of one (i.e., test the application control once) where ITGCs are tested and determined to be effective; else test the application control 25 times
50-250 items in population	10%
< 50 and not weekly, monthly or quarterly	Use judgment, but consider selecting five (5) items or test entire population

### Selecting a Sample

When selecting the sample, the assessment team should follow procedures that ensure the sample is free of any bias or preference. The principal methods for selecting a sample are:

- **Random Selection:** Selection using a structured technique like a random number generator
- **Systematic:** Selecting every nth item
- **Haphazard:** No structured selection technique

In general, random selection is the most unbiased method to use when testing IT controls, although in many instances systematic or haphazard selection might be more appropriate. When using a haphazard approach, it is best to select a purposive sample of a typical instance or other method that provides a sample result that is objective and defensible.

For example, assume an assessment team member is reviewing access privileges granted to users. She obtains a list of all user IDs for an in-scope application, noting that there are 1,500 IDs. By using a random number generator, she identifies 25 numbers between 1 and 1,500. Last, those corresponding user IDs would then be selected from the list of all IDs and review the users for appropriateness of access based upon their job descriptions and responsibilities.

If using systematic selection, the assessment team might divide the population by 25, resulting in 25 groups of 60 items (1,500 / 25 = 60). To establish a starting point the assessment team needs to randomly select a number between 1 and 60. If we assume that the number chosen was 39, the 39th user in the list of 1,500 users would be selected as the first item in the sample. The next item would be the 99th user (39 + 60). The next item would be the 159th user, etc.

An example of where haphazard selection might be an appropriate method is selecting a sample of completed user access request forms to determine if appropriate approvals were obtained before granting access. The population consists of hardcopy documents that have been centrally stored, the size of the population is not known, and there is no numbering system on the forms themselves. In such a situation the assessment team might pull 25 documents at random (haphazardly) from the file.

HITRUST recommends establishing a standardized template for use in documenting the results of sampling-based test procedures. At a minimum, this standardized sampling template should capture the following sampling data points:

- Population source (e.g., the organization's HR system)
- Population size (e.g., 100 terminated employees)
- Population date range (e.g., terminations occurring in calendar year 20XX)
- Minimum required sample size per sampling requirements (e.g., 10 samples)
- Sampling method (random, systematic, or haphazard)
- Procedures performed to ensure the completeness and accuracy of the population

### **Control Exceptions or Deviations**

Dealing with control exceptions or deviations is a matter of judgment. The first step when encountering an exception should be determining what caused the exception. For example, if the assessment team determines that the item causing the exception does not possess the characteristics of the population being tested and should not have been included in the population, selecting a replacement item may be an acceptable approach.

If there is an exception, the assessment team must determine the reason for the exception and determine if it is likely to occur again. If it appears to be an isolated occurrence, the assessment team would document the reason for such a conclusion and can consider selecting and testing additional items (e.g., 15 additional items). Assuming that no further exceptions are encountered, there may be a basis for concluding the control is operating effectively.

An unexpected high rate of exceptions might suggest the control is not operating effectively. The assessment team may then conclude that exceptions similar to the failed item(s) exist in the population and therefore additional testing is not warranted. When such situations exist, identifying alternate controls (see Alternate Control Identification and Selection) may be an option. If alternate controls exist, they can be selected from the CSF where included or submitted to HITRUST's Alternate Controls Committee for approval.

Any exceptions noted by the assessor leading to scores of less than 100% / fully compliant on the policy, procedure, or implemented PRISMA maturity levels should be formally document within the assessor's test results and should be described within MyCSF's "assessor comments" fields.

### **Document findings (Step 7)**

Once controls are assessed through interviews, examination of documentation and testing, the assessment team is in a position to document findings based on the results of these activities, which will ultimately be submitted to HITRUST.

### **Alternate Control Identification and Selection**

The CSF is designed to establish appropriate levels of safeguards related to the protection of sensitive information based on regulatory requirements and risks. It does not take into account environment or situation- specific limitations or circumstances. Given existing infrastructure, technologies and business environments, meeting the CSF

requirements may not always be possible or practical. HITRUST defines a process that allows for alternate controls to provide a means for organizations to meet the requirements of the CSF as they continually improve their security and compliance stance. This process is overseen by the Alternate Controls Committee (ACC) that serves to review, document, approve, and maintain acceptable alternate controls.

### Identifying and Selecting Alternate Controls

Once the initial assessment is completed, the assessment team can return to any non-compliant areas to determine if any alternate controls are identified and documented within the CSF by HITRUST. If so, the assessment team should use the information gathered to determine if the organization or system meets the requirements of the alternate control. If an approved alternate control is implemented with no findings, the gap will be closed.

### Alternate Control Requests

The alternate control request process has been established as a mechanism to allow organizations to address control deficiencies with respect to either organizational or system requirements of the CSF by proposing alternate controls to mitigate the risk.

If no existing approved alternate control exists, or if the existing one(s) are not appropriate for the organization, the control deficiency should be documented and an alternate control proposed through an alternate control request. Alternate control requests should be submitted to [ACC@HITRUSTalliance.net](mailto:ACC@HITRUSTalliance.net), at which point it is assigned a number and tracked by the ACC throughout the review and decision-making process as outlined in the *Risk Analysis Guide for HITRUST Organizations and Assessors*. Once a request is approved or disapproved, the ACC chairperson will notify the submitter and provide the results of the review to HITRUST management. Approved controls will be used in place of the original required controls when the organization submitting the alternate control request undergoes a validated assessment. Approved alternate controls are also available for general use without the need for further consideration by or action from the ACC.

## Reporting and Remediation

### Reporting (Step 8)

#### Develop Remediation Guidance

Following the CSF assessment, the assessment team should develop recommendations to properly treat and manage the identified areas of non-compliance with the CSF. A remediation task should include the suggested steps that the organization should implement to mitigate the risk of an identified gap. A remediation task may consist of process improvements or implementation of technical solutions. The suggested remediation tasks should be formally documented and tailored to the organization's environment.

#### Submit Information to HITRUST

Using MyCSF, the organization or External Assessor—depending on the type of assessment performed: self or validated—submits the completed baseline questionnaire, along with description of scope, overview of the organization's security program, testing performed, and corrective action plans to HITRUST. HITRUST will generate a

CSF Self Assessment, CSF Validated or CSF Validated with Certification report outlining strengths (CSF Validated and Certified only) and potential exposures (all assessments) within the organization's information security program. The report will include a score for each domain in the MyCSF questionnaire. Additional information on the CSF Assurance Program and HITRUST Validated or Validated with Certification reports can be found in the *HITRUST CSF Assurance Program Requirements* document.

### **Socializing the Report**

The CSF assessment of the organization and systems should conclude with the delivery of a report by the external assessor or project coordinator to executive management. If the organization chose to have HITRUST generate the CSF Validated or CSF Validated with Certification report, the project coordinator can use this document. If the organization chose to generate its own report prior to pursuing further reporting from HITRUST, the report document should include the following sections:

- The organization's and business units' level of compliance against the CSF requirements
- The systems' level of compliance against the CSF requirements
- Recommendations to remediate controls,

The report should be socialized with all relevant stakeholders as determined by the project coordinator. A presentation should be made to management and key stakeholders (e.g., business unit coordinators, department directors, system owners) to highlight the assessment and provide an opportunity to discuss the results of the assessment and next steps, if any.

### **Management's Response**

After socialization, management should agree on the specific actions to be taken based on the findings and any recommended remediation guidance. In some cases, an alternate control may be implemented or awaiting approval by HITRUST, or the cost to remediate an issue may greatly exceed the potential risk. Thus, it is possible that no action may be taken based on the recommendation. Ultimately, it is the responsibility of management, not the External Assessor, to approve and implement the appropriate controls.

### **Sharing the Report**

If the organization procured a HITRUST Self Assessment, CSF Validated or CSF Validated with Certification report, the report may be shared with the organization's third parties in accordance with a signed participation agreement.

### **Remediation (Step 9)**

A detailed CAP addressing each identified deficiency or gap should be tracked following the assessment. At a high level, the CAP should reflect management's decisions and contain the following:

- Control Gap Identifier

- Control Gap
- HITRUST CSF Control Mapping
- Point of Contact
- Scheduled Completion Date
- Corrective Actions
- Date Identified
- Status of Corrective Action

The individual(s) responsible for the corrective actions should periodically report back to management to provide status updates, notifications of modifications to the agreed-upon timelines and any other factors that may affect the organization's compliance.

By clearly outlining the remediation effort in a detailed work plan, the organization will have a firm understanding of the scope, timing, roles, and responsibilities of the effort.

### Risk Acceptance

Consistent with NIST SP 800-30 r1, HITRUST allows organizations to accept rather than mitigate control gaps when the control has an average score of three (3) or better, as—given the correlation between maturity and risk—the risk associated with such a control may be considered relatively low. When an organization chooses to accept risk, the analysis submitted in MyCSF to support the selection must show the residual risk for all the requirement statements supporting the control evaluation is less than 20 using the following risk formula:

$$R = L \times I = [(100 - MS) / 100] \times [(IR - 1) \times 25]$$

where, R = risk, L = likelihood, I = impact, MS = HITRUST CSF control maturity score, and IR = impact rating.

For a list of impact ratings for the CSF controls and more information on how risk can be accepted, refer to Appendix A of the *Risk Analysis Guide for HITRUST Organizations and Assessors*, available in the downloads section of the HITRUST website.

**HITRUST<sup>®</sup>**

855.HITRUST

(855.448.7878)

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