**Introduction & Purpose**

The purpose of this document is to define the requirements for those organizations assessing their security and privacy program against the HITRUST CSF or attempting to obtain HITRUST CSF security certification. HITRUST CSF Assessors and those organizations seeking the HITRUST CSF Assessor designation should also refer to this document to ensure adequate understanding of the CSF Assurance Program and related processes.

This document is focused on addressing the process for an organization to assess its internal security and/or privacy programs against the requirements of the HITRUST CSF. The following documents located in the downloads section of the HITRUST website should be referenced for program background and familiarity with the HITRUST CSF:

- HITRUST CSF License Agreement
- HITRUST RMF Whitepaper
- Risk Analysis Guide for HITRUST Organizations and Assessors
- HITRUST CSF Assessment Methodology
- HITRUST CSF Assessor Requirements

**Background**

The HITRUST CSF Assurance Program utilizes a common set of information security and privacy requirements with standardized assessment and reporting processes accepted and adopted by organizations and assessors. Through the HITRUST CSF Assurance Program, organizations and business partners can improve efficiencies and reduce the number and costs of security and privacy assessments.

The HITRUST CSF Assurance Program provides a practical mechanism for validating an organization’s compliance with the HITRUST CSF, an overarching security and privacy framework that incorporates and leverages the existing security and privacy requirements, including federal and international legislation (e.g., ARRA, HIPAA, GDPR), regulatory agency rules and guidance (e.g., NIST, FTC, CMS), state legislation (e.g., Nevada, Massachusetts, Texas), and industry frameworks (e.g., PCI, COBIT).

The standard requirements, methodology, and tools developed and maintained by HITRUST, in collaboration with information security and privacy professionals, enable both relying and assessed entities to implement a consistent approach to third-party compliance management. For the purposes of this document, “relying” and “assessed” will be used as general descriptors, and an “assessed organization” is any organization that undergoes a HITRUST CSF assessment. A “relying party” is any party that accepts a HITRUST CSF Assessment report as an attestation of an assessed organization’s control posture.

Under the HITRUST CSF Assurance Program, organizations can pro-actively or reactively, per a request from a relying entity, perform an assessment against the requirements of the HITRUST CSF. This single assessment will give an organization insight into its state of compliance against the various requirements incorporated into the CSF and can be used in lieu of proprietary requirements and processes for validating third-party compliance.
This program allows for an organization to receive immediate and incremental value from the CSF as it follows a logical path to certification. Unlike other programs, the oversight, vetting, and governance provided by HITRUST means greater industry-wide assurances and security.

### Roles and Responsibilities

The following section describes the roles and responsibilities of each organization in the assessment process, including HITRUST, participating organizations, and approved HITRUST CSF Assessors. Each organization has specific roles with accompanying responsibilities that must be executed for an assessment to be validated or certified by HITRUST.

**HITRUST Alliance, Inc.**

HITRUST Alliance, Inc. serves as the governing organization of the HITRUST CSF. HITRUST Alliance, Inc.’s responsibilities include:

- Maintaining and updating the HITRUST CSF based on feedback from HITRUST CSF Assessors and participating organizations.
- Supporting HITRUST CSF Assessors and participating organizations in interpreting HITRUST CSF control objectives, specifications, requirements, assessment procedures, risk factors, and standards/regulations cross-references.

**HITRUST Services Corporation**

HITRUST Services Corp (“HITRUST”) provides the guidance, oversight, validation, and certification for the CSF Assurance Program. HITRUST’s responsibilities in the assessment validation and certification process include:

- Approving assessor organizations and accrediting and training organizations and individuals who perform CSF assessments and/or assist participating organizations in implementing the HITRUST CSF.
- Sharing knowledge of security threats/vulnerabilities as well as successful mitigation strategies as provided by HITRUST CSF Assessors and participating organizations.
- Developing and providing approved assessment methodologies and tools for HITRUST CSF Assessors and participating organizations.
- Issuing final validation or certification reports based on the HITRUST CSF Assessors’ findings, and identification of required corrective actions as appropriate.

**Participating Organizations**

HITRUST participating organizations are those organizations that have adopted the HITRUST CSF as their security, privacy, and compliance framework for use internally and/or by third parties. Under the HITRUST CSF Assurance Program, a HITRUST participating organization’s responsibilities include:

- Coordinating the performance of assessments and implementing corrective actions and organizational transformations as necessary.
• Funding its HITRUST CSF Assurance Program work, including assessments for validation and/or certification and corrective actions, performed by internal and external resources where required.
• Maintaining the information security management program that has been validated or certified through continuous monitoring, continuous review, and periodic re-assessments.
• Communicating actual or suspected data breaches involving the assessed environment to HITRUST.

Additionally, all organizations must have a mechanism to report to regulatory agencies; a HITRUST CSF Assessment Report is one way for organizations to meet such requirements.

Qualified Resources
HITRUST requires partner organizations and the individuals of partner/participating organizations to meet certain thresholds before receiving approval to perform HITRUST CSF-related work, including assessments, certifications, and remediation.

HITRUST defines three classifications of qualified resources:

- **Authorized HITRUST CSF 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.

- **HITRUST Certified CSF Practitioner (CCSFP)** is a designation reserved for individuals who have completed the CCSFP training course, passed the certification exam, and meet the required background and experience requirements necessary to effectively use the HITRUST CSF. Such individuals typically work for a HITRUST CSF 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 CSF assessment engagements, have completed the CHQP training course, and have passed the CHQP certification exam. Such individuals typically work for a HITRUST CSF Assessor organization.

HITRUST also defines three specific roles within a CSF Assessor’s Validation Assessment team, all of which are subject matter experts in the field of information security and/or privacy and are holders of HITRUST-issued certifications:

- The **Engagement Executive** is the CCSFP who owns the relationship between the CSF Assessor firm and the assessed entity. This individual is expected to review and approve the engagement scope, the test plan, testing results, and testing documentation.

- The **Engagement Lead** is the CCSFP responsible for the creation and execution of the test plan, performing/overseeing sampling, analyzing test results, leading walkthroughs and interviews, and coordinating the validated assessment’s day-to-day fieldwork.

- The **Quality Assurance Reviewer** is a CHQP who ensures that engagement execution meets internally defined and HITRUST-defined quality assurance requirements, including adequacy and completeness of the working papers, appropriate treatment of exceptions, and proper definition and application of scoping decisions.
Details on the specific requirements and process of becoming a qualified resource can be found in section 3 of the *HITRUST CSF Assessor Requirements* document.

**CSF Assurance Program Overview**

The HITRUST CSF Assurance Program enables trust in information protection through an efficient and manageable approach by identifying incremental steps for an organization to take on the path to becoming HITRUST CSF Validated or HITRUST CSF Certified.

The comprehensiveness of the security and privacy requirements for the assessed entity is based on the multiple levels within the HITRUST CSF as determined by defined risk factors. The level of assurance for the overall assessment of the entity is based on multiple tiers, from self-assessments to validation by on-site testing performed by an authorized HITRUST CSF Assessor. The results of the assessment are documented in a standard report with remediation activities tracked in corrective action plans (CAPs). Once vetted by HITRUST, the assessed entity can use the assessment results to report to external parties in lieu of existing security or privacy reporting processes, saving time and containing costs.

The diagram below outlines the relationship between comprehensiveness of the assessment and the level of assurance provided by the assessment for organizations of varying complexity based on the risk of the relationship as determined by the relying organization:

A HITRUST CSF assessment allows an organization to communicate to relying entities its compliance with the HITRUST CSF and the NIST Cybersecurity Framework, and optionally with other requirements such as GDPR, PCI, MARS-E, and many others. HITRUST reviews the assessment results and CAPs to provide added assurance to the external entities relying on the assessed entity's results.
The HITRUST CSF Assurance Program effectively establishes trust in information protection through an achievable assessment and reporting path for organizations of all sizes, complexities, and risks. The HITRUST CSF Assurance Program operates at two levels: Self Assessment and Validated Assessment. Certification is awarded to organizations that complete a validated assessment and meet the requisite scoring threshold and other certification criteria. The sections below describe general considerations when performing a self or a validated assessment. Please refer to the HITRUST CSF Assessment Methodology for more detailed guidance.

**CSF Assessments**

A HITRUST CSF assessment provides organizations with a means to assess and communicate their current state of security and compliance with external entities along with CAPs to address any identified gaps. An organization can, using the services of a HITRUST CSF Assessor or performing a self-assessment, conduct an assessment against the HITRUST CSF and have the results reported by HITRUST under the HITRUST CSF Assurance Program. The assessed entity is not required by HITRUST to meet all the security and privacy control requirements contained within the HITRUST CSF. Instead, HITRUST CSF assessments provide the assessed entity and the relying entity with a snapshot into the current state of security, privacy, and compliance of the assessed entity.

The level of assurance the assessed entity, and/or the relying entity on behalf of the assessed entity, has chosen determines the assessment strategy: self-assessment or validated assessment. As suggested by the name, a validated assessment provides a higher level of assurance since it includes independent and on-site third-party testing of controls, providing a more complete picture of security, privacy, and compliance to both the assessed entity and the relying entity.

**Scope**

Assessment scoping is the process of identifying the specific organizational business units, physical locations, systems, and other elements to be included in the CSF assessment. The scope will depend on the resources, security and privacy program maturity, and risk tolerance of an organization.

For organizations with standard operating procedures deployed consistently across the enterprise, HITRUST recommends selecting representative samples of assets for review versus testing every asset. For example, if the organization uses a standard operating system configuration, the CSF Assessor would only need to review a statistically relevant sample. However, in organizations where security or privacy control consistency is lacking, the HITRUST participating organization and HITRUST CSF Assessor may determine that a review of all in-scope assets is required for certification.

Organizations undergoing a CSF validated assessment are required to prepare a verbose description of the system(s) and process(es) included in the assessment. This scope description should be written with as much detail about the system(s) and process(es) as possible and include descriptions of the service offering(s) and/or product(s) they support. Items to include in the scope description include component parts, internal vs. external development, connectivity, interfaces, and a high-level network or architecture diagram. It should also communicate if the environment as
assessed as a whole, or, if partially assessed, what exclusions existed. This scope description should include a scope overview designed to communicate the assessment’s scoping elements in summary form. HITRUST encourages the use plain English and not industry insider-only language when describing the scope of an assessment; if uncommon acronyms must be used, they should be spelled out. While defining assessment scope is the responsibility of the assessed entity, the formal description of scope that is submitted to HITRUST for inclusion in the final assessment report should be jointly prepared through collaboration between the assessor and the assessed entity.

Additional resources to reference when scoping the assessment include the HITRUST CSF Assessment Methodology document.

**Self-Assessments**

Organizations may choose to self-assess using the standard methodology, requirements, and tools provided under the HITRUST CSF Assurance Program. Neither HITRUST nor a third-party performs any validation on the results of the self-assessment.

Using HITRUST’s MyCSF tool, the organization being assessed first completes a risk-based scoping questionnaire that drives control selection and assessment scope based on general, organizational, geographical, systematic, and regulatory risk factors. Upon completion of the scoping questionnaire, a customized set of HITRUST CSF control references and requirement statements is generated in the MyCSF tool. The organization then enters responses for each requirement statement and determines the level of compliance for each of the following five (5) PRISMA-based maturity levels:

- Is a **policy** or standard in place?
- Is there a **process or procedure** to support the policy?
- Has it been **implemented**?
- Is it being **measured** and tested by management to ensure it is operating?
- Are the **measured** results being managed to ensure corrective actions are taken as needed?

For each maturity level, the organization indicates its level of compliance. The five options are:

- Non-compliant (0%)
- Somewhat compliant (25%)
- Partially compliant (50%)
- Mostly compliant (75%)
- Fully compliant (100%)

Once the organization has determined and entered compliance scores for each PRISMA maturity level across all requirement statements, it submits the populated MyCSF object to HITRUST for report generation.
HITRUST CSF Validated Assessments

HITRUST CSF validated assessments can be leveraged by organizations of any size or complexity and consist of more rigorous on-site testing performed by an authorized HITRUST CSF assessor. The decision to undergo an on-site HITRUST CSF validated assessment should be based on the risk of the relationship between the assessed entity and the relying entity. For example, where two parties share a large amount of sensitive information, and/or the connectivity and access is high in relation to the number of systems and the risk of those systems, an on-site HITRUST CSF validated assessment may be necessary to provide a higher level of assurance to both parties. In cases where the HITRUST CSF validated assessment determines that the assessed entity meets all the security and/or privacy control requirements for HITRUST CSF certification, it will receive a validated assessment report with certification.

An on-site assessment also utilizes HITRUST’s MyCSF tool. As was the case for a self-assessment, the entity being assessed would begin by completing the risk-based scoping questionnaire in the MyCSF tool. Upon completion of the scoping questionnaire, a comprehensive and customized set of HITRUST CSF control references and requirement statements will be generated. The entity being assessed responds to the requirement statements based upon the PRISMA maturity model, ensuring that they are answered accurately. Once the organization has determined and entered compliance scores for each PRISMA maturity level across all requirement statements, it submits the populated MyCSF object to its Assessor for validation.

Validation Procedures

HITRUST CSF Assessors are required to perform a sufficient level of on-site walkthroughs and testing of control documentation to: (a) confirm / validate the assessed entity’s self-identified scoring levels / responses, and (b) to ensure that compliance gaps have been appropriately identified.

CSF requirement statements that are required for HITRUST CSF certification must be validated and are done so through a variety of testing strategies. This is to provide assurance to those relying entities that the control is in fact implemented and operating effectively. Procedures performed by CSF Assessors during validated assessment fieldwork include:

- On-site walkthroughs and/or interviews of personnel to verify that policies and procedures are documented and implemented.
- Inspection of written CSF-relevant policies and procedures to ensure sufficient coverage of CSF requirements.
- Observation of the performance or existence of relevant controls and control processes.
- Inspection of documentation evidencing the existence / performance of relevant controls, including inspection of documentation associated with samples.
- Performance of technical testing to validate the implementation or operation of relevant controls.
- Inspection of operational or independent measures or metrics used by the organization.
- Inspection of evidence generated by mechanisms used by the organization to manage relevant controls.
These testing strategies are consistent with the guidance provided by the National Institute of Standards and Technology (NIST) as outlined in their Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*. Although the most appropriate testing strategy and the extent of testing can be a matter of judgment, HITRUST CSF Assessors must ensure that both are consistent with the guidance provided by HITRUST and the illustrative procedures included in MyCSF.

Any previous/recent reviews or assessments covering the scope of the HITRUST CSF assessment can and should be used by the HITRUST CSF Assessor to assist in the review and testing process; however, any third-party reports that are relied upon in lieu of testing should not be more than one year old. This one-year reliance threshold is determined using the date of the 3rd party audit’s final report or final memo as compared to the start date of the validated assessment effort. Care should be taken to ensure adequate scope coverage of any third-party reports being relied upon.

All testing performed by the HITRUST CSF Assessor in support of the validated assessment must be conducted within 90 days of the submission date to HITRUST. All control processes, system configurations, implemented tools, written policies, and written procedures should be in operation / established for at least 90 days in order to be considered by the assessor during the validated assessment effort. Reliance on testing beyond this 90-day threshold, on controls in operation less than 90 days, or on written policies and procedures in existence for less than 90 days requires HITRUST approval prior to submission.

Additional guidance on conducting a validated assessment and testing can be found in the HITRUST CSF Assessment Methodology document.

**Test Plan**

During the planning phase of a validated assessment effort, the HITRUST CSF Assessor must prepare a test plan which outlines the anticipated testing of all applicable / in-scope requirement statements; it serves as the blueprint for the performance of the validated assessment. The test plan shouldn’t be a straight copy and paste repeat of the illustrative procedures defined by HITRUST. While helpful, these haven’t been tailored enough to the match the specifics of the client’s environment or to be quickly followed by team members in the field. Instead, the test plan should be based on the HITRUST-provided illustrative procedures associated with each PRISMA maturity level of each applicable / in-scope CSF requirement statement. The test plan should also include details on any sampling that is used for testing (e.g., how the sample will be selected, population source, etc.). Test plans should also identify who in the Authorized CSF Assessor organization will act as the Engagement Executive, QA Reviewer, and Engagement Lead and should be signed-off by the Engagement Executive, Engagement Lead and optionally by the QA Reviewer before fieldwork commences. The test plan is not complete unless test steps have been drafted for all PRISMA attributes across all in-scope requirement statements. Unless certain PRISMA attributes for specific requirement statements have been specifically excluded from the scope of testing, each PRISMA attribute needs a test procedure prepared (in such case, a scoping note to that effect should be included in the test plan).
Areas that need to be understood by the CSF Assessor prior to developing a test plan include:

- The systems, business processes, and physical locations to be assessed.
- The risk factors to be assessed against.
- The nature of populations from which samples will be pulled (e.g., users, endpoints, network devices, mobile devices).
- Any CSF requirement statements which may have a shared responsibility.

**Working Papers**

CSF Assessors must create working papers from artifacts collected during the validated assessment which were used to support the CSF Assessor’s agreement with the assessed entity’s scoring / responses. Each working paper must include the following markup:

- The name of the assessment.
- The name of the person that tested the working paper.
- The date the working paper was tested.
- A description of the associated test procedure.
- The result of the associated test procedure.
- (Optional best practice) The date the evidence / artifact was created or pulled from the source system (e.g., in the form of a date stamp clearly visible in the log, report, screenshot, etc. being examined).
- (Optional best practice) A clear identification of the associated scoping elements (e.g., systems, facilities, business units) being tested in that working paper.

These working paper markup elements are not specifically required for written policies and procedure workpapers. However, including markup in these documents can help them stand on their own and can benefit reviewers, the client, and subsequent assessor teams.

Note that a validated assessment’s collective body of working papers is considered incomplete if validation of only a portion of an assessment’s scope is reflected in the working papers. For example, working papers which include screenshots from only one of the two in-scope applications’ configurations would be rejected during HITRUST’s quality assurance checks.

All working papers created by an assessor in the course of a validated assessment must be uploaded by the assessor into MyCSF. As documents are being uploaded, assessors are expected to consistently link each to the related requirement statement as well as the related PRISMA maturity attribute(s) (e.g., implemented). MyCSF features several edit checks associated with uploading workpapers. For example, any requirement statements scored as mostly compliant or fully compliant in the policy and process attributes must have documents linked to those attributes.
Sampling
CSF Assessors are often required to perform sampling in order to validate management’s self-scoring. 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

When performing sampling tests featuring homogeneous supporting evidence, assessor teams are not required to add the electronic markup to every sample item’s markup. For the sake of efficiency, when supporting evidence is homogeneous, assessor teams need only to add the required electronic markup to one sample item’s workpaper.

Additional information regarding the performance of sampling can be found in the HITRUST Assurance Methodology document.

Documenting Exceptions noted by the CSF Assessor in the course of validated assessment fieldwork should be captured in MyCSF’s “Assessor Comment” fields to enable reviewers—such as the CSF Assessor’s QA Reviewer, the Engagement Lead, the Engagement Executive, and HITRUST’s QA function—to easily reconcile to PRISMA maturity levels, corrective action plans, and working papers. Any conditions noted by the CSF Assessor necessitating a change in scoring should be discussed and agreed with management of the assessed entity. 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.

Pre-submission Quality Assurance Review
Prior to submitting a validated assessment to HITRUST for review and report assembly, the assessor’s engagement executive as well as a Certified HITRUST Quality Professional (CHQP) within the assessor firm is required to perform a quality assurance review of the assessment’s documentation. This pre-submission QA review should be driven by and documented through the HITRUST CSF Assessor Quality Checklist available for download within MyCSF as well as on the HITRUST website. This review generally focuses on whether the HITRUST CSF Assurance program requirements outlined in this document as well as in the HITRUST CSF Assurance Methodology document were observed. When performing his/her review, a CHQP’s review considerations include areas such as:

- Have all required documents (listed in Appendix B of this document) been populated and uploaded into MyCSF?
- Where validation procedures outlined in the test plan reflective of the requirement statements’ illustrative procedures. For example, was a sample selected if the illustrative procedure called for sampling?
- Where applicable, were sampling attributes clearly documented, including the basis for the selection of the population, the method of sample selection?
- Do facts presented in the client comments, assessor comments, and working papers support the scoring levels indicated by the entity and agreed upon by the assessor team?
- Is the timesheet in MyCSF reflective of the actual hours worked by the assessor team?
- Have all timing requirements, such as validated assessment procedures being performed within 90 days of submission date, been observed?

**Submitting Results to HITRUST**

Refer to Appendix B for the documents to be submitted to HITRUST following an on-site validated assessment.

**HITRUST CSF Certified**

“HITRUST CSF Certified” refers to an organization that has met all CSF certification requirements as defined by HITRUST based on industry input and analysis. “CSF Certification” involves performance of a Validated assessment leveraging the MyCSF tool, the embedded HITRUST CSF control requirement statements, and the PRISMA maturity model. CSF certification provides relying entities with greater assurance that an assessed entity is appropriately managing risk. CSF certification is designed to remove the variability in acceptable security and privacy requirements by establishing a baseline defined by industry, removing unnecessary and costly negotiations and risk acceptance. In being HITRUST CSF Certified, an organization is communicating to its business partners and other third-party entities (e.g., regulatory agencies) that protection of sensitive information is both a necessity and priority, that essential security and privacy controls are in place, and that management is committed to information security and privacy.

**Granting Certification**

The decision for granting certification to an organization is based on the testing results of the HITRUST CSF Assessor and ultimately reviewed, approved, and certified by HITRUST. To be HITRUST CSF Certified, the organization must:

- Successfully demonstrate meeting all controls in the CSF required for the current year’s certification at the appropriate level required for the organization based on its responses to the MyCSF requirement statements.
- Achieve a rating of 3+ or higher on HITRUST’s scale of 1 to 5 for each of the 19 domains documented in MyCSF. (Note that under certain circumstances organizations may be CSF Certified with a 3 rating in one or more domains. In these instances, the risk must be inherently low and corrective action plans must be documented in the report.)

Where certification is granted, certification is valid for 2 years (24 months) from the certification date on the condition that the interim assessment and continuous monitoring requirements are met.
The development of the HITRUST CSF and requirements for certification continually evolve to account for new regulatory requirements, standards, environmental changes, technologies, and vulnerabilities. Because of this, certifications are designated by the CSF version to distinguish the CSF versions and certification requirements applicable. Please refer to Appendix A for a complete list of the current CSF controls required for certification.

HITRUST CSF Certifications contain the wording “meets the HITRUST CSF vX Certification Criteria”. The scope of certification is included on the Letter of Certification and further defined in the report to provide details on the organization’s systems covered by the assessment. It is up to HITRUST’s discretion as to whether multiple certificates are issued in circumstances where multiple systems are certified.

**De-certification**

Upon discovery or suspicion of a data security breach, the compromised entity must notify HITRUST. HITRUST CSF Certified entities that experience an actual or suspected data security breach will undergo an investigation initiated by HITRUST and at the entities’ expense with an Approved HITRUST CSF Assessor organization of HITRUST’s choosing to evaluate the nature of the breach. If the breach is deemed to be material to the entity’s certification (for example, a control failure by the HITRUST CSF Certified organization for a required control, or a misrepresentation of a required control by either the HITRUST CSF Assessor or HITRUST CSF Certified organization), the certification will be suspended. Inmaterial breaches not related to the required controls of the CSF will not result in suspension of the certification or de-certification.

For the HITRUST CSF Certified status to be reinstated by HITRUST, the compromised entity must perform an analysis of the breach, which shall include a forensics analysis if the breach resulted in whole or in part due to a failure of technical controls. The results of the analysis, accompanied by a detailed CAP specific to the incident, must be submitted to HITRUST for review. After successful completion of the plan, the compromised entity must bring in an Approved HITRUST CSF Assessor to review and assess the corrective actions and provide any findings to HITRUST. If no gaps are noted, the HITRUST CSF Certified status will be reinstated for the compromised entity.

For a two-year period following the breach, the compromised entity will be re-assessed annually following the original assessment process and include all HITRUST CSF controls.

**Interim Assessment**

For an entity to retain its certification for a two-year period, an interim assessment must be completed and submitted to HITRUST in the 90 day window leading up to the one year anniversary of the certification issuance date. For MyCSF subscribers, the interim assessment is generated automatically 90 days prior to the required submission date. Customers can also manually generate the object 120 days prior. All interim assessments for objects using CSF version 9.1 or later are required to be performed in MyCSF.

The following steps outline what HITRUST expects of the CSF Assessor during an interim assessment:

- Ask the assessed entity to update the MyCSF object that was the basis for the initial assessment.
- Review the updated MyCSF object with management of the assessed entity and note any changes to the environment and control requirement responses.
• For each of the 19 assessment domains, discuss with the owner(s) any changes noted or verify that no changes had occurred.

• Where a significant change to a domain or control requirement has occurred, determine its impact and test the new/updated control. For example, if the client implemented a new email encryption tool, test the new tool to ensure it is operating and the settings are appropriate.

• Perform full testing/validation procedures for 19 requirement statements (1 per domain) randomly selected by the MyCSF tool, working with the assessed entity to re-score these requirement statements in MyCSF if necessary, based on the results of the test procedures performed. These validation procedures documented in the MyCSF tool in the organization’s Interim Assessment Object. Note that all assessor expectations related to timing of validation procedures, performance of validation procedures, and creation of working papers apply equally to validated assessments (although a test plan is not required).

• Review the status of CAPs that were included in the initial assessment report and conclude as to whether the entity is making satisfactory progress. This is also documented in the MyCSF tool in the organization’s Interim Assessment Object.

• Within the MyCSF tool, document indicate whether there have been significant changes, whether adequate progress was made on the CAPs and a recommendation as to whether or not the assessed entity should retain its certification.

• Submit the Interim Assessment Object to HITRUST for its review. If HITRUST concludes that the assessed entity should retain its certification, it will issue a letter to the entity that indicates its certification is still valid. If HITRUST concludes that it no longer meets the requirements, a letter will be sent to the entity asking it to remove any references to its HITRUST certification from its literature and website.

The interim assessment will be submitted to HITRUST by the Assessor. Upon receipt, HITRUST then performs the same level of quality assurance checks as performed on a validated assessment submission.

Any acquisition of one entity or by another entity must be communicated to the HITRUST CSF Assessor immediately so that the scope and significance can be evaluated and communicated to HITRUST. Should a re-assessment be necessary, HITRUST will designate the assessed entity’s HITRUST CSF Certified status as pending until the results of the re-assessment confirm that the changed environment continues to meet the requirements set forth.

**Re-assessments**

The purpose of the re-assessment is to validate the assessed entity is continuing to comply with the controls of the required HITRUST CSF controls required for certification. HITRUST requires that assessed entities conduct a complete re-assessment every second year. Re-assessments could occur sooner pending evaluation of a data security breach or significant change in the organization’s operating environment as determined by the HITRUST CSF Assessor’s professional judgment. For example, a full re-assessment may be required annually for an organization that is expanding operations (naturally or through mergers and acquisitions) or changing its environment and systems extensively and rapidly. In no event shall the interval between re-assessments exceed 24 months. The process for the re-assessment will follow the original assessment process specified under the HITRUST CSF Assurance Program.
Corrective Action Plan

The Corrective Action Plan (CAP) prepared by the assessed entity describes the specific measures that are planned to correct compliance gaps identified during the assessment for validation or certification. HITRUST understands that most organizations have more vulnerabilities than they have resources to address. Organizations should prioritize corrective actions based on the security and/or privacy category of the information systems, the direct effect the vulnerability has on the overall security and privacy posture of the information systems, and the requirements for HITRUST CSF certification.

The CAP should include, at a minimum, a control gap identifier, a description of the compliance gap, CSF requirement statement mapping, remediation owner, scheduled completion date, planned corrective action(s), and status. The HITRUST CSF Assessor should review the CAP to evaluate the effectiveness of the remediation strategy, and provide any recommendations to the assessed entity. CAPs are only required for validated reports with certification and must be submitted to HITRUST within 30 days of the organization receiving a copy of the draft report.

Continuous Monitoring

Once an assessed entity has had its assessment certified by HITRUST, the entity enters a critical post-assessment period called continuous monitoring. While assessment and re-assessments are important to measure the implementation of security and privacy controls and compliance status at a point in time, they are not sufficient to ensure ongoing compliance and effective security between assessments and reviews.

Assessed entities must implement a continuous monitoring program to determine if the controls implemented in accordance with the HITRUST CSF continue to remain effective over time given the dynamic threat environment and that any identified gaps are remediated in accordance with the CAP.

HITRUST recommends continuous monitoring programs include configuration management for all information systems, security, and privacy risk analysis for planned or actual changes to an operational environment or an information system, ongoing selective evaluation of security and privacy controls, and frequent interaction between information systems management and the security and privacy teams.

HITRUST requires that security and privacy documentation (e.g., policies, procedures) and the CAP are updated frequently to reflect changes to the environment, systems and/or security and privacy posture of the organization.
## Appendix A: HITRUST CSF v9.2 Certification Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01.a</td>
<td>Information Security Management Program</td>
</tr>
<tr>
<td>01.b</td>
<td>User Registration</td>
</tr>
<tr>
<td>01.c</td>
<td>Privilege Management</td>
</tr>
<tr>
<td>01.d</td>
<td>User Password Management</td>
</tr>
<tr>
<td>01.e</td>
<td>Review of User Access Rights</td>
</tr>
<tr>
<td>01.h</td>
<td>Clear Desk and Clear Screen Policy</td>
</tr>
<tr>
<td>01.j</td>
<td>User Authentication for External Connections</td>
</tr>
<tr>
<td>01.l</td>
<td>Remote Diagnostic and Configuration Port Protection</td>
</tr>
<tr>
<td>01.m</td>
<td>Segregation in Networks</td>
</tr>
<tr>
<td>01.n</td>
<td>Network Connection Control</td>
</tr>
<tr>
<td>01.o</td>
<td>Network Routing Control</td>
</tr>
<tr>
<td>01.q</td>
<td>User Identification and Authentication</td>
</tr>
<tr>
<td>01.t</td>
<td>Session Timeout</td>
</tr>
<tr>
<td>01.v</td>
<td>Information Access Restriction</td>
</tr>
<tr>
<td>01.w</td>
<td>Sensitive System Isolation</td>
</tr>
<tr>
<td>01.x</td>
<td>Mobile Computing and Communications</td>
</tr>
<tr>
<td>01.y</td>
<td>Televworking</td>
</tr>
<tr>
<td>02.a</td>
<td>Roles and Responsibilities</td>
</tr>
<tr>
<td>02.d</td>
<td>Management Responsibilities</td>
</tr>
<tr>
<td>02.f</td>
<td>Disciplinary Process</td>
</tr>
<tr>
<td>02.i</td>
<td>Removal of Access Rights</td>
</tr>
<tr>
<td>03.b</td>
<td>Performing Risk Assessments</td>
</tr>
<tr>
<td>03.c</td>
<td>Risk Mitigation</td>
</tr>
<tr>
<td>03.d</td>
<td>Risk Evaluation</td>
</tr>
<tr>
<td>04.a</td>
<td>Information Security Policy Document</td>
</tr>
<tr>
<td>04.b</td>
<td>Review of the Information Security Policy</td>
</tr>
<tr>
<td>05.a</td>
<td>Management Commitment to Information Security</td>
</tr>
<tr>
<td>05.h</td>
<td>Independent Review of Information Security</td>
</tr>
<tr>
<td>05.i</td>
<td>Identification of Risks Related to External Parties</td>
</tr>
<tr>
<td>05.j</td>
<td>Addressing Security When Dealing with Customers</td>
</tr>
<tr>
<td>05.k</td>
<td>Addressing Security in Third-Party Agreements</td>
</tr>
<tr>
<td>06.c</td>
<td>Protection of Organizational Records</td>
</tr>
<tr>
<td>06.d</td>
<td>Data Protection and Privacy of Covered Information</td>
</tr>
<tr>
<td>06.e</td>
<td>Prevention of Misuse of Information Assets</td>
</tr>
<tr>
<td>06.g</td>
<td>Compliance with Security Policies and Standards</td>
</tr>
<tr>
<td>06.h</td>
<td>Technical Compliance Checking</td>
</tr>
<tr>
<td>07.a</td>
<td>Inventory of Assets</td>
</tr>
<tr>
<td>07.c</td>
<td>Acceptable Use of Assets</td>
</tr>
<tr>
<td>08.b</td>
<td>Physical Entry Controls</td>
</tr>
<tr>
<td>08.d</td>
<td>Protecting against External and Environmental Threats</td>
</tr>
<tr>
<td>08.j</td>
<td>Equipment Maintenance</td>
</tr>
<tr>
<td>08.l</td>
<td>Secure Disposal or Re-Use of Equipment</td>
</tr>
<tr>
<td>09.b</td>
<td>Change Management</td>
</tr>
<tr>
<td>09.c</td>
<td>Segregation of Duties</td>
</tr>
<tr>
<td>09.e</td>
<td>Service Delivery</td>
</tr>
<tr>
<td>09.f</td>
<td>Monitoring and Review of Third-Party Services</td>
</tr>
<tr>
<td>09.g</td>
<td>Controls Against Malicious Code</td>
</tr>
<tr>
<td>09.k</td>
<td>Controls Against Mobile Code</td>
</tr>
<tr>
<td>09.l</td>
<td>Equipment Maintenance</td>
</tr>
<tr>
<td>09.m</td>
<td>Network Controls</td>
</tr>
<tr>
<td>09.n</td>
<td>Security of Network Services</td>
</tr>
<tr>
<td>09.o</td>
<td>Management of Removable Media</td>
</tr>
<tr>
<td>09.p</td>
<td>Disposal of Media</td>
</tr>
<tr>
<td>09.q</td>
<td>Information Handling Procedures</td>
</tr>
<tr>
<td>09.s</td>
<td>Information Exchange Policies and Procedures</td>
</tr>
<tr>
<td>09.v</td>
<td>Electronic Messaging</td>
</tr>
<tr>
<td>09.y</td>
<td>On-line Transactions</td>
</tr>
<tr>
<td>09.aa</td>
<td>Audit Logging</td>
</tr>
<tr>
<td>09.ab</td>
<td>Monitoring System Use</td>
</tr>
<tr>
<td>09.ad</td>
<td>Administrator and Operator Logs</td>
</tr>
<tr>
<td>10.a</td>
<td>Security Requirements Analysis and Specification</td>
</tr>
<tr>
<td>10.b</td>
<td>Input Data Validation</td>
</tr>
<tr>
<td>10.f</td>
<td>Policy on the Use of Cryptographic Controls</td>
</tr>
<tr>
<td>10.h</td>
<td>Control of Operational Software</td>
</tr>
<tr>
<td>10.k</td>
<td>Change Control Procedures</td>
</tr>
<tr>
<td>10.l</td>
<td>Outsourced Software Development</td>
</tr>
<tr>
<td>10.m</td>
<td>Control of Technical Vulnerabilities</td>
</tr>
<tr>
<td>11.a</td>
<td>Reporting Information Security Events</td>
</tr>
<tr>
<td>11.c</td>
<td>Responsibilities and Procedures</td>
</tr>
<tr>
<td>11.d</td>
<td>Learning from Information Security Incidents</td>
</tr>
<tr>
<td>12.b</td>
<td>Business Continuity and Risk Assessment</td>
</tr>
<tr>
<td>12.c</td>
<td>Developing and Implementing Continuity Plans Including Information Security</td>
</tr>
<tr>
<td>12.d</td>
<td>Business Continuity Planning Framework</td>
</tr>
</tbody>
</table>
Appendix B: CSF Onsite Assessment Submission Documents

CSF Assessors are required to ensure that the following documentation has been completed / included within MyCSF for all validated assessment submissions:

- A completed MyCSF Assessment Object.
- A test plan.
- The Organizational Overview and Scope (template located in MyCSF).
- A “Management Representation Letter” from the assessed entity, a copy of which can be found in “Documents” section of each assessment in MyCSF.
- The “Participation Agreement” signed by the assessed entity, a copy of which can be found in “Documents” section of each assessment in MyCSF.
- A completed “HITRUST CSF Assessor Quality Checklist”, signed and initialed by the assessor Engagement executive and QA reviewer.
- A completed assessor timesheet within MyCSF.
- 100% of working papers. These working papers must meet the minimum working paper requirements documented in the CSF Assurance Program Documentation Requirements.