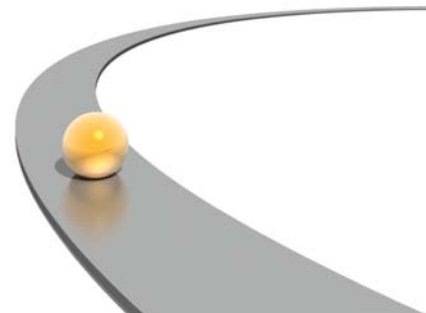


# HITRUST

## CSF Assurance Program Requirements

---

2010 — Version 1.3



## Table of Contents

1 Introduction .....	4
1.1 Purpose .....	4
1.2 External References .....	4
1.3 Background .....	4
1.4 Roles and Responsibilities .....	5
1.4.1 HITRUST, LLC .....	5
1.4.2 HITRUST Services Corporation .....	5
1.4.3 Member organizations .....	6
1.4.4 Qualified Resources .....	6
2 CSF Assurance Process .....	7
2.1 Overview .....	7
2.2 Assessment .....	8
2.2.1 Scope .....	8
2.2.4 Testing Strategy .....	8
2.3 CSF Validated .....	9
2.3.1 Self Assessment .....	9
2.3.2 Remote .....	9
2.3.3 On-site .....	10
2.4 CSF Certified .....	11
2.4.1 Testing .....	11
2.4.2 Granting Certification .....	11
2.4.3 De-certification .....	12
2.4.4 Annual Review .....	13
2.4.5 Re-assessments .....	13

3 Corrective Action Plan..... 15

4 Continuous Monitoring..... 16

Appendix A – 2010 Certification Requirements..... 17

## **1 Introduction**

### **1.1 Purpose**

The purpose of this document is to define the requirements for those seeking an assessment or certification of their security program against the Common Security Framework (CSF) to be validated by HITRUST under the CSF Assurance Program. CSF Assessors and those organizations seeking the CSF Assessor designation should also refer to this document to ensure adequate understanding of the process and applicable requirements.

### **1.2 External References**

The following HITRUST documents located on HITRUST Central in the “Downloads” section should be referenced for program background and familiarity with the CSF, as this document specifically addresses the process for organizations to assess their internal security program for validation by HITRUST:

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

### **1.3 Background**

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

The CSF Assurance Program provides a practical mechanism for validating an organization’s compliance with the Common Security Framework (CSF), an overarching security framework that incorporates and leverages the existing security requirements of healthcare, including federal (e.g., ARRA and HIPAA), state, third party (e.g., PCI and COBIT) and government (e.g., NIST, FTC and CMS).

The standard requirements, methodology and tools developed and maintained by HITRUST, in collaboration with healthcare and information security professionals, enables both relying and assessed entities to implement a consistent approach to third-party compliance management. Under the CSF Assurance Program, organizations can proactively or reactively, per a request from a relying entity, perform an assessment against the requirements of the CSF. This single assessment will give an organization insight into its state of compliance against the various requirements incorporated into the CSF to 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 in healthcare and other industries, the oversight, vetting and governance provided by HITRUST and the CSF Assurance Committee means greater industry-wide assurances and security.

## **1.4 Roles and Responsibilities**

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

### **1.4.1 HITRUST, LLC**

HITRUST, LLC serves as the governing organization of the CSF. HITRUST, LLC's responsibilities include:

- Supporting CSF Assessors and member organizations in interpreting CSF control objectives, specification, requirements, assessment procedures, risk factors and standards/regulations cross-references.
- Maintaining and updating the CSF based on feedback and industry collaboration.

### **1.4.2 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:

- Accrediting and training organizations and individuals who perform the assessments and assist member organizations in implementing the CSF.
- Sharing knowledge of security threats/vulnerabilities as well as successful mitigation strategies as provided by CSF Assessors and member organizations.
- Developing and providing approved assessment methodologies and tools for member CSF Assessors and member organizations.
- Issuing final validation or certification based on the CSF Assessor's (or member organization's where permitted) findings, report, and corrective action plan.

### 1.4.3 Member organizations

HITRUST member organizations are those organizations that have adopted the CSF as the security and compliance framework used internally and/or for third parties. Under the CSF Assurance Program, a HITRUST member organization's responsibilities include:

- Coordinating the performance of assessments and implementing corrective actions and organizational transformations as necessary.
- Funding its CSF Assurance 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 data breaches to HITRUST in accordance with the requirements of The Department of Health and Human Services.

For the purposes of this description "relying" and "assessed" will be used as general descriptors. While covered entities can generally be classified as relying and business associates as assessed, there are many instances where a covered entity is also a business associate with its own security requirements that it must meet as mandated by its customers. Additionally, all organizations must have a mechanism to report to state and federal agencies and subsequently must perform an assessment.

### 1.4.4 Qualified Resources

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

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

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

CSF Practitioners is a designation reserved for individuals who, as part of a CSF Assessor organization or a HITRUST member organization (e.g., a hospital), have the background, experience, training and understanding to effectively use the CSF. Because CSF Practitioners can be individuals employed by any type of organization, use of the CSF is not limited to performing internal/external assessments. The CSF may also be used as a reference for developing, revising, or maintaining a comprehensive security and compliance program.

Details on the specific requirements and process of becoming a qualified resource can be found in the HITRUST CSF Assessor Requirements.

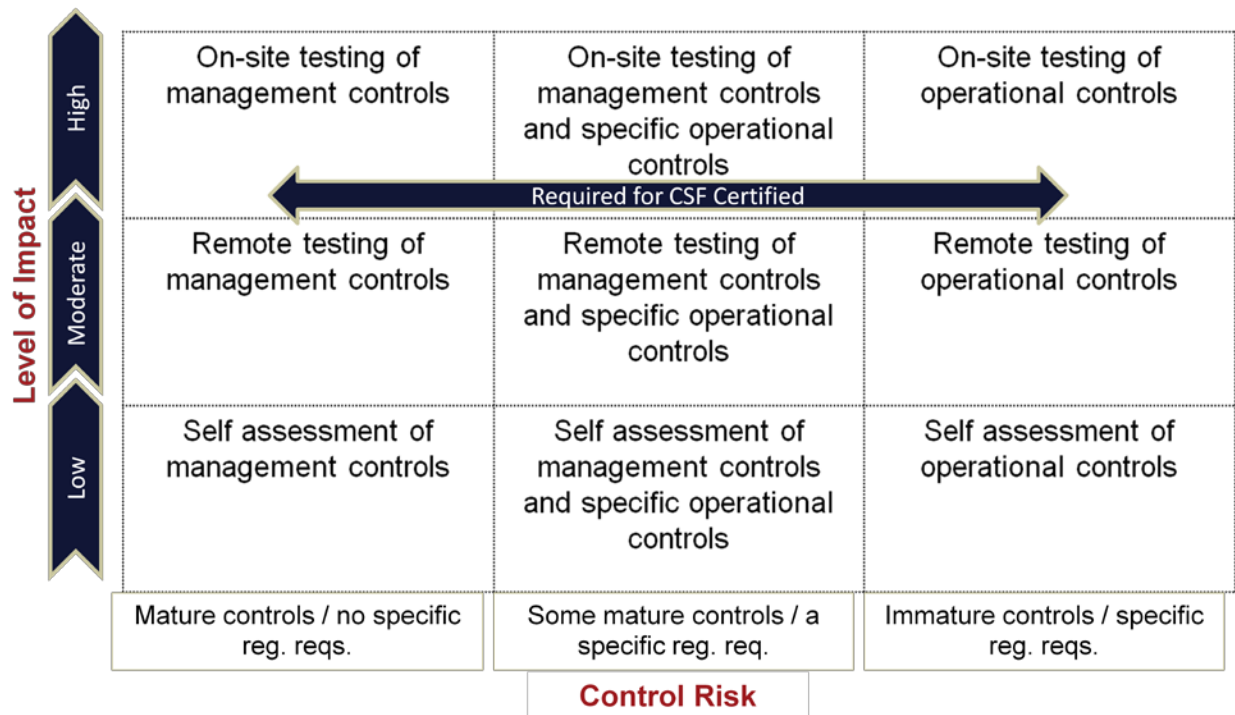
## 2 CSF Assurance Process

### 2.1 Overview

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

The comprehensiveness of the security requirements for the assessed entity is based on the multiple levels within the 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-assessment questionnaires to remote interview/review and on-site analysis/testing performed by a CSF Assessor. The results of the assessment are documented in a standard report with a compliance scorecard and remediation activities tracked in a corrective action plan (CAP). Once vetted by HITRUST and performed for all levels of assurance, the assessed entity can use the assessment results to report to external parties in lieu of existing security requirements and processes, saving time and containing costs.

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



## 2.2 Assessment

The assessment allows the organization seeking a validated assessment to determine and communicate to relying entities its compliance with the entire CSF, among other requirements such as HIPAA and HITECH. HITRUST validates the assessment and CAP to provide assurance to the external entities relying on the assessed entity's results.

The CSF Assurance Program effectively establishes trust in health information protection through an achievable assessment and reporting path for organizations of all sizes, complexities and risks. CSF Assurance is provided at two levels: CSF Validated and CSF Certified.

The sections below describe general considerations when performing an assessment for either CSF Validated or CSF Certified purposes. Please refer to the HITRUST CSF Implementation and Assessment Methodology for more detailed guidance.

### 2.2.1 Scope

The scope of the assessment will depend on the resources, security 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 assessor would only need to review a statistically relevant sample size for the review. However, in organizations where security control consistency is lacking, the HITRUST member organization and CSF Assessor may determine that a review of all in-scope assets is required to effectively prepare for certification.

Sampling of systems during testing is permitted. For more information please refer to the *Implementation and Assessment Methodology* document. Sample of business or organizational units is not permitted.

### 2.2.4 Testing Strategy

HITRUST requires those controls that are required for certification be validated through various testing strategies. This is to provide assurance to those relying entities that the control is in fact implemented and operating effectively. These strategies include examining documentation, interviewing organization personnel, and testing system configurations. These strategies are consistent with the guidance provided by the National Institute of Standards and Technology as outlined in their Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*. It is ultimately up to the expert judgment of the CSF Assessor to determine the most appropriate testing strategy and the extent of testing to be performed to gain the level of assurance required (see sections 2.3.2 and 2.3.3 for more information).

## 2.3 CSF Validated

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

For CSF Validated assessments, 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, remote validation, or on-site validation. Each increases the level of assurance chosen and includes more rigorous testing that more thoroughly assesses security controls and identifies deficiencies, providing a more complete picture of security and compliance to both the assessed entity and the relying entity.

### 2.3.1 Self Assessment

Organizations may choose to self assess using the standard methodology, requirements, and tools provided under the CSF Assurance Program. HITRUST will perform limited validation on the results of the self assessment to provide a limited level of assurance to the relying entity without undue burden on the assessed entity.

HITRUST will supply the assessed entity with a questionnaire aligned with the compliance requirements of the healthcare industry and scaled appropriately to the small size and limited complexity of the organization.

The validation of the self assessment performed by HITRUST will consist of spot checking the questionnaire for accuracy to ensure that it is answered completely and that ambiguous or incomplete responses are addressed. The supporting documentation associated with each question will be reviewed to ensure it is sufficient to meet the security control requirements and that any missing documentation is noted.

### 2.3.2 Remote

The choosing of a remote 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 moderate amount of information, some of which is sensitive, or the connectivity and access is moderate in relation to the number of systems and the risk of those systems, the risk of this relationship can be classified as moderate and a remote CSF Validated assessment should be sufficient to provide assurance to both parties.

The remote assessment consists of a questionnaire aligned with the compliance requirements of the healthcare industry. Additional testing is performed by a third party CSF Assessor that is

trained and accredited by HITRUST. The CSF Assessor will support the completion of the questionnaire to ensure that it is answered accurately in accordance with the requirements of the CSF. The CSF Assessor will review any supporting documentation associated with the questions and CSF requirements to ensure it is sufficient to meet the security control requirements, and that any missing documentation is gathered or noted as a gap. The CSF Assessor will remotely, via telephone, interview security personnel of the assessed entity to further validate that the policies and procedures documented are implemented and followed. Any previous reviews/assessments should be used by the CSF Assessor to identify strengths and weaknesses; however it is ultimately up to the professional judgment of the CSF Assessor to determine the quality of the tests and whether or not they can comfortably rely on the results for validation. The CSF Assessor will perform an external vulnerability scan of the assessed entity's network environment. Any identified technical vulnerabilities are to be noted in the final report to HITRUST.

Once the assessment is complete, a report, comprehensive CAP, and compliance scorecard are to be documented in accordance with the tools and templates provided by HITRUST.

The completed questionnaire, assessment work papers, supporting documentation, and corrective actions are sent to HITRUST for review and final validation. Once validated by HITRUST, the assessed entity may, as permitted by HITRUST, share the assessment results consisting of the findings report, compliance scorecard and CAP with third party relying entities.

### **2.3.3 On-site**

On-site CSF Validated assessments are permitted for organizations of any size or complexity, and consist of more rigorous testing on-location at the entity. The choosing of an on-site 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, the risk of this relationship can be classified as high and an on-site CSF Validated assessment is necessary to provide assurance to both parties.

The on-site assessment consists of a questionnaire aligned with the compliance requirements of the healthcare industry. Additional testing will be performed by a third party CSF Assessor that has been trained and accredited by HITRUST. The CSF Assessor will validate the completion of the questionnaire and ensure that it is answered accurately in accordance with the requirements of the CSF. The CSF Assessor will review any supporting documentation associated with the questions and CSF requirements to ensure it is sufficient to meet the security control requirements and that any missing documentation is gathered or noted as a gap. The CSF Assessor will interview security personnel of the assessed entity to verify that the policies and procedures documented are implemented and followed. Any previous reviews/assessments should be used by the CSF Assessor to identify strengths and weaknesses; however it is ultimately up to the professional judgment of the CSF Assessor to determine the quality of the tests and whether or not they can comfortably rely on the results for validation. The CSF Assessor will perform internal and external vulnerability scans of the assessed entity's network environment. Any identified technical vulnerabilities are to

be noted in the final report to HITRUST. As required by the CSF, the CSF Assessor will test system configurations to verify that the technical requirements of the CSF are implemented and adhered to.

Once the assessment is complete, a report, comprehensive CAP, and compliance scorecard are to be documented in accordance with the tools and templates provided by HITRUST.

The completed questionnaire, assessment work papers, supporting documentation, and corrective actions are to be sent to HITRUST for review and final validation. Once validated by HITRUST, the assessed entity may, as permitted by HITRUST, share the assessment results consisting of the findings report, compliance scorecard and CAP with third party relying entities.

## **2.4 CSF Certified**

CSF Certified is a means of confirming that an organization has met all of the certification requirements of the CSF as defined by HITRUST based on industry input and analysis. CSF certification leverages the same components of CSF validation but provides relying entities with greater assurance that their third parties are appropriately managing risk. CSF certification is designed to remove the variability in acceptable security requirements by establishing a baseline defined by the healthcare industry and to be used for the healthcare industry, removing unnecessary and costly negotiations and risk acceptance. By being CSF Certified, an organization is communicating to their business partners and other third-party entities (e.g., state or federal agencies) that sensitive information protection is both a necessity and priority; essential security controls are in place, management is committed to information security, and the risk of a breach has been reduced to an acceptable level.

### **2.4.1 Testing**

The assessed entity seeking certification will engage a third party HITRUST Qualified CSF Assessor to perform the assessment. The assessment shall be performed in accordance with the guidance set forth in the HITRUST Implementation and Assessment Methodology and will use the same processes and tools as the on-site CSF Validated assessment. An organization does not have to meet those Implementation Requirements where regulatory risk factors are the only drivers of an increased level of control. For example, if the organization is subject to PCI requirements, and the level 3 Implementation Requirement of control 01.xx is driven only by *Subject to PCI Compliance*; the organization can be certified WITHOUT meeting the requirements specified in this level for this control.

### **2.4.2 Granting Certification**

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

The following are the CSF Certified documentation requirements to be submitted by the CSF Assessor to HITRUST:

- A summary of assessment duration.
- Acknowledgement that all actions were performed in accordance with HITRUST policies, procedures, and applicable requirements, listing those individuals who performed the assessment with sign-off from the most senior, active member of the team.
- The scope of the assessment including organizational entities/business units, systems, and the risk determination factors for each control as defined by the CSF.
- An audit trail, including documentation, interview notes, testing results, and prior assessments/reviews if used.
- Successful demonstration of all applicable controls in the CSF as required for the current year's certification (either as stated or through alternate controls approved by HITRUST).
- A report that describes the findings of the assessment with reference to the CSF control specification and CAP.
- A CAP for all non-compliant findings.
- A compliance scorecard referencing each CSF control specification and the applicable regulatory requirements including, but not limited to, HIPAA and HITECH.

Where certification is granted, certification is valid for two years from the certification date as it appears on the certificate where the continuous monitoring requirements are met.

The development of the CSF and requirements for certification are expected to evolve to account for new regulatory requirements, standards, environmental changes, technologies, and vulnerabilities. Because of this, certification will be designated by the year received to distinguish the CSF version and certification requirements applicable. Please refer to *Appendix A* for a complete list of the CSF control specifications required for certification.

The CSF Certified certificate granted will contain the wording *"meets the [YEAR] criteria of HITRUST: Specification for healthcare information security management"*. The scope of certification will be recorded on the certificate providing details on the organization's entities/business units and systems covered by the assessment. It is up to HITRUST's discretion as to whether multiple certificates will be issued in circumstances where multiple entities/business units are certified, or whether one certificate shall specify all certified components of the assessed entity.

### **2.4.3 De-certification**

CSF Certified entities that experience a data security breach, by which there is actual or suspected compromise of PHI (regardless of volume), will have their CSF Certified status suspended.

Upon discovery of a data security breach, the compromised entity must notify HITRUST in accordance with the breach notification requirements of the Department of Health and Human Services.

For the CSF Certified status to be reinstated by HITRUST, the compromised entity must perform a forensics analysis. The results of the forensics 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 a CSF Assessor to review and assess the corrective actions and provide any findings to HITRUST. If no gaps are noted, the 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 including all CSF controls.

#### **2.4.4 Annual Review**

To ensure the assessed entity continues to meet the CSF certification requirements and is remediating any previously identified gaps, HITRUST requires that a CSF Assessor normally conducts a review annually of the assessed entity. The review will address the continuous monitoring activities and CAP developed by the organization. In order to remain CSF Certified, the organization must demonstrate reasonable progress towards the activities identified in the CAP.

The assessed entity must inform the CSF Assessor of any significant changes in its business policies, practices, processes and controls, particularly if such changes might affect the organization's ability to continue meeting the required CSF certification security control requirements. Such changes may merit the need for a more extensive re-assessment of the organization and systems. If the CSF Assessor becomes aware of such a change in circumstances, it is the responsibility of the CSF Assessor to report these findings to HITRUST, which will determine whether a re-assessment is needed. The evaluation will take into account the following:

- The nature and complexity of the entity's operations
- The frequency of changes to the entity's operations
- The relative effectiveness of the entity's monitoring and change management controls for ensuring continued compliance with the CSF certification security control requirements

Any acquisition of one entity or by another entity must be communicated to the 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 CSF Certified status as pending until the results of the re-assessment confirm that the changed environment meets the requirements set forth.

The CSF Assessor will document and provide to HITRUST a report containing findings, if any, towards the CAP.

#### **2.4.5 Re-assessments**

The purpose of the re-assessment is to validate the assessed entity is continuing to comply with the controls of the required CSF Certified controls.

HITRUST requires that assessed entities conduct a complete re-assessment every second (2<sup>nd</sup>) year. This amount of time could decrease pending a data security breach or significant change in the organization's operating environment as defined by the 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 CSF Assurance Program.

### 3 Corrective Action Plan

The corrective action plan (CAP) prepared by the assessed entity, and the CSF Assessor as applicable, describes the specific measures that are planned to correct deficiencies 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 category of the information systems, the direct effect the vulnerability has on the overall security posture of the information system, and requirement for CSF certification.

The CAP should include, at a minimum, a weakness identifier, description of the weakness, CSF control mapping, point of contact, resources required (dollars, time, and/or personnel), scheduled completion date, milestones with completion dates, changes to milestones, how the weakness was identified (assessment, assessor, date), current status, comments, and risk level. The CSF Assessor must review the CAP to evaluate the effectiveness of the remediation strategy, provide recommendations, and document any findings to be submitted to HITRUST.

## 4 Continuous Monitoring

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

Assessed entities need to implement a continuous monitoring program to determine if the controls implemented in accordance with the 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 risk analysis for planned or actual changes to an operational environment or an information system, ongoing selective evaluation of security controls, and frequent interaction between information system management and the security team.

HITRUST requires that security documentation (e.g., policies, procedures) and the CAP are updated frequently to reflect changes to the environment, systems and/or security posture of the organization.

The security team and information system owner(s) should report progress made during the remediation process and are encouraged to report to HITRUST any innovative or successful measures taken when remediating gaps.

## Appendix A – 2010 Certification Requirements

The top issues the industry identified as resulting in the most severe breaches and loss of covered information are:

- Insecure and/or unauthorized removable transportable media and laptops (internal and external movements)
- Insecure and/or unauthorized external electronic transmissions of covered information
- Insecure and/or unauthorized remote access by internal and third party personnel
- Insider snooping and data theft
- Malicious code and inconsistent implementation and update of prevention software
- Inadequate and irregular information security awareness for the entire workforce
- Lack of consistent network isolation between internal and external domains
- Insecure and/or unauthorized implementation of wireless technology
- Lack of consistent service provider, third party and product support for information security
- Insecure web development and applications
- Ineffective password management and protection
- Improper sanitization and disposal of electronic and hardcopy media

In consideration of the above issues, the Control Specifications of the CSF that are required for 2010 Certification are:

<b>Required for HITRUST Certification 2010</b>	
01.a Access Control Policy	06.e Prevention of Misuse of Information Assets
01.b User Registration	06.g Compliance with Security Policies and Standards
01.d User Password Management	07.c Acceptable Use of Assets
01.f Password Use	08.l Secure Disposal or Re-Use of Equipment
01.h Clear Desk and Clear Screen Policy	09.aa Audit Logging
01.i Policy on Use of Network Services	09.ab Monitoring System Use
01.j User Authentication for External Connections	09.ac Protection of Log Information
01.m Segregation in Networks	09.ae Fault Logging
01.n Network Connection Control	09.af Clock Synchronization
01.o Network Routing Control	09.c Segregation of Duties
01.q User Identification and Authentication	09.e Service Delivery
01.r Password Management System	09.f Monitoring and Review of Third Party Services
01.v Information Access Restriction	09.g Managing Changes to Third Party Services
01.w Sensitive System Isolation	09.j Controls Against Malicious Code

01.x Mobile Computing and Communications	09.m Network Controls
01.y Teleworking	09.o Management of Removable Media
02.a Roles and Responsibilities	09.p Disposal of Media
02.d Management Responsibilities	09.q Information Handling Procedures
02.e Information Security Awareness, Education, and Training	09.s Information Exchange Policies and Procedures
04.a Information Security Policy Document	10.b Input Data Validation
04.b Review of the Information Security Policy	10.f Policy on the Use of Cryptographic Controls
05.a Management Commitment to Information Security	10.l Outsourced Software Development
05.b Information Security Coordination	10.m Control of Technical Vulnerabilities
05.i Identification of Risks Related to External Parties	11.a Reporting Information Security Events
05.k Addressing Security in Third Party Agreements	11.c Responsibilities and Procedures