Leveraging HITRUST CSF Assessment Reports
A Guide for New Users
Universal Agreement that the Current Model for Third Party Assurance is Broken

- There are no scenarios where performing 15, 50 or 250 or more unique assessments makes sense for a business associate to communicate their information privacy and security posture (given the same breadth and depth of the assessments)
- Nor does it make sense to maintain and support organization-specific assessment methodologies and multiple assessments for each organization
- HITRUST has been working with healthcare organizations and business partners to identify a practical and implementable approach

Covered Entity Challenges with Third Party Assurance

- Complex contracting process due to organization-specific security requirements
- Low rate, inaccurate and incomplete responses
- Inadequate due diligence of questionnaires
- Difficulty monitoring the status and effectiveness of corrective action plans
- Difficulty tracking down appropriate contacts at business associate
- Costly and time-intensive data collection, assessment and reporting processes
- Inability to proactively identify and track risk exposures at business associate
- Lack of visibility into downstream risks related to business associate (i.e., business associate’s own business partners)
- Lack of consistent reporting to management on business associate risks

Business Associate Challenges with Third Party Assurance

- Complex contracting process due to unique security requirements
- Broad range and inconsistent expectations for responses to questionnaires—inability to effectively leverage responses across organizations
- Complex processes:
  - Maintaining broad range of reporting requirements
  - Tracking to varied expectations around corrective action plans
  - Tracking down appropriate contacts for customers
  - Expensive and time-intensive audits by customers
  - Inability to consistently and effectively report to and communicate with customers
  - Risk exposure to inconsistent responses from different business units of the business associate

Complex processes:
- Maintaining broad range of reporting requirements
- Tracking to varied expectations around corrective action plans
- Tracking down appropriate contacts for customers
- Expensive and time-intensive audits by customers
- Inability to consistently and effectively report to and communicate with customers
- Risk exposure to inconsistent responses from different business units of the business associate
HITRUST CSF-based Third Party Assurance

HITRUST CSF

- Developed in collaboration with health care and security professionals
- Provides healthcare organizations a certifiable standard/framework with a comprehensive, flexible and consistent approach to regulatory compliance and risk management
- Helps organizations demonstrate a reasonable standard of due care and due diligence
- Due to continual updates and improvements it has become the most widely adopted framework used within the healthcare industry
- [https://hitrustalliance.net/hitrust-csf/](https://hitrustalliance.net/hitrust-csf/)

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 program, healthcare organizations and their business associates can improve efficiencies and reduce the number and costs of security assessments
- The oversight and governance provided by HITRUST supports a process whereby organizations can trust that their third parties have essential security controls in place
- [https://hitrustalliance.net/csf-assurance/](https://hitrustalliance.net/csf-assurance/)
The HITRUST CSF Assurance Program Validated Assessment Report

Is based on …

• A common set of controls based on existing standards/regulations
• An established, industry-accepted baseline of security requirements
• Requirements prioritized by industry input and data breach analyses
• A standard set of assessment questionnaires, tools, and processes
• Specific risk factors that help tailor controls to the assessed organization
• An independent assessment by a HITRUST CSF Assessor

Provides organizations with …

• Standard report, compliance scorecard, and corrective action plan (CAP) formats for the industry
• Assurance there are minimal gaps in required controls for CSF certified entities
• Oversight and governance by HITRUST
• HITRUST validation of assessment results & remediation activity (CAPs)
• Reduced risk and compliance exposure
• Increased assurances around data protection for third parties
Our target audience

- Focus of the presentation is on consumers of a HITRUST CSF Assurance Program Validated Report ("Report") with little or no familiarity with the HITRUST CSF and CSF Assurance Program, which includes:
  - Staff/management reviewing a third party’s HITRUST Report to determine the level of risk incurred by providing access to the organization’s information, and
  - Regulators reviewing an organization’s HITRUST Report for statutory and regulatory compliance
- May also be used by an organization’s workforce members who may be unfamiliar with the HITRUST CSF and CSF Assurance Program but need to understand what a HITRUST Report says about their own organization’s information protection program

What we want to accomplish

Allow an organization’s management or staff to understand and leverage a HITRUST Report to meet their specific requirements for third party assurance.

What we’ll cover

1. What the report contains
2. What the information means
3. How it describes an organization’s security posture
4. How you can align it with your current approach
5. Where you can find more information
Section 1

WHAT THE REPORT CONTAINS
1. HITRUST Background

The Health Information Trust Alliance (HITRUST) was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with healthcare, business, technology and information security leaders, has established the HITRUST CSF, a customizable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information. Beyond the establishment of the HITRUST CSF, HITRUST is also driving the adoption of and reciprocal certifications in the framework and sound risk management practices through awareness, education, advocacy, and outreach activities. For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit www.HITRUSTAlliance.net.

An integral component to achieving HITRUST’s goal to advance the healthcare industry’s protection of health information is the establishment of a practical mechanism for validating an organization’s compliance with the HITRUST CSF.

The HITRUST CSF is an evolving security framework that incorporates and leverages the existing security requirements (e.g., HIPAA) of healthcare organizations, including federal (e.g., HIPAA and NIST), state (e.g., COI and C2), and other government agencies (e.g., NIST, ITIC, and CMS). The HITRUST CSF—healthcare’s model implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity—is already being widely adopted by leading healthcare players, providers, and data exchanges as their security framework.
2. Letter of Certification*

January 30, 2016
Assessed Entity
Address
City, State and ZIP

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an approved HITRUST CAS Assurance Partner to validate such information, and HITRUST’s independent confirmation that the work was performed in accordance with the HITRUST CAS Assurance Program, the following business units of the organization meet the 2016 HITRUST CAS Certification Criteria:

Assessed Entity: Further explanation of assessed entity/Subsequent entity letters

The certification is valid for a period of two years assuming the following occurs:

- A continuous monitoring program is in place to determine if the controls continue to operate effectively over time
- No data security breach reported to a federal or state agency by law or regulations has occurred
- No significant changes in the business or security policies, practices, contexts, and processes have occurred that might impact its ability to meet the HITRUST CAS certification criteria
- Annual program testing (e.g., scans) identified in the Corrective Action Plan (CAP)
- Timely completion of the interim review as defined in the HITRUST CAS Assurance Program Requirements

The Health Information Trust Alliance (HITRUST) has developed the HITRUST CAS, a certification framework that provides organizations with the needed structure, detail and clarity relating to information security offered to the healthcare industry. HITRUST, with input from leading organizations within the industry, identifies a subset of the HITRUST CAS control requirements that an organization must be HITRUST CAS Certified. For those HITRUST CAS control requirements that are not currently being met, the organization must have a CAP that reflects its plans for meeting such requirements.

Additional information on the HITRUST CAS Certification program can be found at the HITRUST website: www.HITRUSTAlliance.net

HITRUST
855.HITRUST
www.HITRUSTAlliance.net

Copyright 2016 HITRUST Alliance. All Rights Reserved.

* Or Letter of Validation

3. Representation Letter

January 30, 2016
HITRUST LLC
6666 North Spring Blvd.
Suite 120
Las Vegas, NV 89143

In connection with our engagement to perform an assessment of Assessed Entity’s security controls compared with the HITRUST CAS controls required for certification, we recognize that obtaining representations from you concerning the information contained in this report and the information regarding your security controls is a significant procedure in enabling us to complete your portion of the engagement. Accordingly, we make the following representations to you and the recipients of your report regarding our security controls which are true to the best of our knowledge and belief:

- We acknowledge that, as members of management, we are responsible for the controls implemented to secure protected health information (PHI) as required by HIPAA and HITRUST’s CAS certification program.
- We have performed fully all organizational tasks during the engagement.
- We have made available to the HITRUST CAS Assurance Provider all records and necessary documentation related to the control-related processes used to protect PHI processed by the systems included in the scope of this engagement.
- We have disclosed all design and operation changes in our controls over PHI for which we are aware, including those for which we believe the cost of corrective action may exceed the benefits.
- No events or transactions have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing this certification report.

We understand that the engagement was conducted in accordance with the security requirements contained in the HITRUST CAS. We also understand that the sufficiency of this report and the procedures performed is solely the responsibility of report recipients.

Very truly yours,

Author’s Signature

4. Assessment Context

Prepared for
Assessed Entity
Address
City, State and ZIP

Contact
Name
Email address

Date of Report
January 25, 2016

Type of Assessment
Onsite OR remote including
- Evaluation of controls and processes
- Review and testing of technical systems

Company Background
and description of the current and the protocols provided or requested

Number of Employees
Nature

Geographic Scope of Operations
State / Multi state / Off-shore (Outside U.S.)

Organizational Risk Factors
- Selection of business factors
- Number of records processed, etc.
- State Regulatory or Privacy

Regulatory Risk Factors
- Selection of regulatory factors
- HIPAA, etc.

System Risk Factors
- Processes and controls in place, etc.
- Processes and frameworks, etc.

HITRUST
855.HITRUST
www.HITRUSTAlliance.net

© 2016 HITRUST Alliance. All Rights Reserved.
5. Scope of the Assessment

6. Security Program Analysis

7. Assessment Results
8. Overall Security Program Summary

8.1. Overview

The HITRUST Security Program is designed to provide a comprehensive approach to security and privacy protection. The program is based on the HITRUST CSF (Control Security Framework) and includes controls for information security, risk management, and compliance.

The program is structured into multiple domains, each of which is focused on a specific area of security. These domains are

- Domain 1: Information Security
- Domain 2: Risk Management
- Domain 3: Compliance
- Domain 4: Legal

Each domain includes specific controls that are designed to address the risks associated with that domain.

8.2. Control Areas

The controls are organized into control areas, which are the basic building blocks of the CSF. Each control area is focused on a specific aspect of security.

- Control Area 1: Threat Assessment
- Control Area 2: Risk Management
- Control Area 3: Policy and Procedures
- Control Area 4: Controls Implementation
- Control Area 5: Monitoring and Assessments
- Control Area 6: Risk Response

Each control area includes specific controls that are designed to address the risks associated with that area.

8.3. Control Implementation

The controls are implemented through a combination of policies, procedures, and technical controls. The implementation is designed to ensure that the controls are effective in protecting the organization's information assets.

The implementation process includes:

- Identification of controls
- Development of policies and procedures
- Configuration and testing of technical controls
- Ongoing monitoring and assessment

8.4. Monitoring and Assessment

The monitoring and assessment process is designed to ensure that the controls are effective in protecting the organization's information assets. The process includes:

- Regular assessments and audits
- Continuous monitoring of key indicators
- Remediation of identified deficiencies

The monitoring and assessment process is critical to ensuring that the organization's security posture remains robust and effective.

9. Breakdown of Controls Required for Certification by Assessment Domain

The required controls for certification identified in the HITRUST CSF reflect the control needed to address the most common sources of breaches for the industry. An organization must demonstrate a level of each of the control description domains (control area) to qualify for certification. In fewer circumstances, a level 5 analysis is required in the gap analysis project. Ordinary is a further display of a control to the rest of the environment. The industry rating is based on the survey results of organizations that have undergone a third-party validated assessment.
Appendix A – Testing Summary

Below is a summary of the documentation reviewed, personnel interviewed and technical testing performed or reviewed for the controls outlined in the Security Questionnaire and HITRUST CSF.

Documentation:
- Acceptable Use Policies
- Information Protection Policies
- Password Security Policies
- Remote Access Policies
- Physical Security Policies
- Personnel Security Policies
- additional policies and procedures

Interviews:
- John Smith – Internal Audit
- James Bond – Information Management
- Steve Rogers – Security Administration/Verification
- Operational Report – Windows Security
- additional client personnel

Technical Testing:
- Vendor Audits – Field of Competence & Performance
- Client Interoperability Scan Report, August 2015
- Client Security Service Verification Audit – August 2015
- Vendor 2: Audit Verification – Random Sample
- Client Workstation AV Report, August 2015
- additional testing or reviews of peer testing

Appendix B – Corrective Action Plan

HITRUST requires that an organization written a Corrective Action Plan (CAP) for any HITRUST CSF Certification controls not met at a Level 2 HITRUST score. Certification CAPs identify CSFs needed to obtain or maintain certification. Additional CAPs are not required but documented to ensure complete implementation. For general recommendations on areas of improvement, please refer to Section 8.

<table>
<thead>
<tr>
<th>Control Area</th>
<th>Corrective Actions</th>
<th>Status</th>
<th>N/A Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1.1.0101</td>
<td>remediation plan</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>A.2.1.0201</td>
<td>remediation plan</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>A.2.1.0202</td>
<td>remediation plan</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>A.3.1.0203</td>
<td>remediation plan</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>A.4.1.0204</td>
<td>remediation plan</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>A.5.1.0205</td>
<td>remediation plan</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

... Table continues in the next report.

HITRUST
855.448.7878
www.HITRUSTAlliance.net

© 2016 HITRUST Alliance. All Rights Reserved.
Appendix C – Questionnaire Results

Appendix D – System Profile
Section 2

WHAT THE INFORMATION MEANS
Cover Page

- Not much to say here … it’s a cover page
- But it does provide:
  - The name of the entity that’s the subject of the assessment report
  - The date of the report, which tells you how long the report is valid, i.e., date of the report + 2 years

1. HITRUST Background

- This section simply provides a brief overview of the HITRUST Alliance and the information protection framework, the CSF, upon which the report is based
- For more information, you can refer to the following resources:
  - www.hitrustalliance.net

2. Letter of Certification*

- This letter from HITRUST states the entity that was assessed meets all the requirements for HITRUST CSF certification
  - Provides the organization’s name and date of certification (consistent with the cover page)
  - Specifies the certification is good for 2 years if certain conditions are met
- *If certification requirements aren’t met, then a letter stating the assessment has been validated by HITRUST is included instead

3. Representation Letter

- This letter is from the organization that was the subject of the validated assessment
- It basically provides attestation from the organization that they
  - Are responsible for the controls,
  - Have responded to the assessor in good faith and that nothing has been misrepresented, and
  - They foresee nothing that might adversely impact the assessment results
- Any misrepresentation by the entity could cause HITRUST to invalidate the report
4. Assessment Context

- This section provides additional information about the organization, e.g.:
  - Entity name and address
  - Background information
  - Point of contact for the assessment
- It also provides information about the assessment, including:
  - Assessment type (e.g., 3rd party / validated)
  - Specific risk factors used to tailor the CSF controls to the entity
  - For more information on scoping & tailoring: https://hitrustalliance.net/documents/assurance/csf/CSFAssessmentMethodology.pdf

Risk Factors

- Risk factors support (1) the “flexibility of approach” allowed under the HIPAA Security Rule and (2) NIST’s concept of tailoring a specified set of controls, referred to as a control baseline, to meet an entity’s needs
- HITRUST uses three (3) types of risk factors to help provide a tailored “fit”
  - Organizational – generally the amount of ePHI held/processed
  - System – additional risks posed by a system, e.g., allowing access through an Internet connection or the number of interfaces it may have
  - Regulatory – Applicable compliance requirements, e.g., credit cards

5. Scope of the Assessment

- An overview of the assessed entity and the industry segment within which it operates
- The services / products provided by the entity
- Primary systems placed in scope of the assessment with description of the platforms, their functions and the PHI involved
- Any services within scope of the report that are outsourced to a third party
- Additional information about the scope of the report, such as business units and/or processes included

6. Security Program Analysis

- This section is intended to provide the reader with a concise summary of the assessed entity’s
  - Information protection program
  - Information protection organization
- It also provides detailed information on
  - The security and privacy tools and technology the entity deploys in the scoped environment
  - Relevant independent assessments by internal audit and/or external consulting and professional services firms (e.g., for a PCI audit or a vendor’s penetration test of the corporate perimeter)
7. Assessment Results

- Organizations must generally implement all requirements in all 135 CSF controls (or 149 if privacy requirements are included) as tailored by its applicable risk factors and any subsequent risk analysis to:
  - Provide a complete set of reasonable and appropriate controls
  - Address all reasonably anticipated threats
  - Provide adequate protection of ePHI, and subsequently
  - Minimize risk at an acceptable level

- However, consistent with NIST guidelines ([http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)), “organizations can use targeted risk assessments, in which the scope is narrowly defined, to produce answers to specific questions … or to inform specific decisions…”

- HITRUST CSF validated assessments provide a reasonable level of assurance at a reasonable cost by selecting specific:
  - High risk controls (based on an analysis of breach data and subject matter expert input)
  - High interest controls (designed to minimally address each HIPAA Security Rule standard and implementation specification, including the standard on risk analysis)

- The 2016 CSF Assurance Program requires the assessment of 66 CSF controls for the purposes of certification and basic third party assurance

- This section lets the reader of the report identify which of these 66 controls meet or do not meet certification requirements, whether a CAP is required, and the specific identifier for the weakness/CAP.

- For more information on HITRUST’s risk vs. compliance-based approach to information protection and the overall approach to supporting attestations of HIPAA compliance, refer to [https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf](https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf) & [https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf](https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf)
8. Overall Program Summary

- This is boilerplate that presents the 15-point scale used by HITRUST to communicate the maturity of a control’s implementation
  - Controls are evaluated using a 5-level maturity model
  - HITRUST scores the controls
  - HITRUST converts the scores to a 15-point rating for the purpose of CSF certification
- For more information, refer to: https://hitrustalliance.net/documents/csf_rmf RELATED/RiskAnalysisGuide.pdf

[5-level Control Maturity Model]

Assurance the control has been properly implemented is indicated by:
1. **Policy** (25 pts) – Does an organization know what it’s supposed to do?
2. **Process** (sometimes referred to as Procedures) (25 pts) – Does the organization know how to do what it’s supposed to do?
3. **Implemented** (25 pts) – Does the organization implement all the elements of a specified control and does it implement it everywhere it’s supposed to be implemented?

Assurance the control will continue to be effective is indicated by:
4. **Measured** (15 pts) – Does the organization monitor the effectiveness of the control?
5. **Managed** (10 pts) – Does the organization correct any problems that are identified while monitoring the effectiveness of the control?

Maturity Scoring Approach

- Compliance with a maturity level’s requirements is indicated by:
  - **Non-compliant** (NC, 0%) – Very few if any of the control requirements are implemented for the maturity level assessed (e.g., Policy)
  - **Somewhat Compliant** (SC, 25%) – Some of the control requirements are implemented for the maturity level assessed (e.g., Policy)
  - **Partially Compliant** (PC, 50%) – About half of the control requirements are implemented for the maturity level assessed (e.g., Policy)
  - **Mostly Compliant** (MC, 75%) – Many of the control requirements are implemented for the maturity level assessed (e.g., Policy)
  - **Fully Compliant** (FC, 100%) – Most if not all of the control requirements are implemented for the maturity level assessed (e.g., Policy)
- Scores are computed as the sum of the points awarded for each level

15-point Rating Scheme for Certification

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>1-</th>
<th>1+</th>
<th>2-</th>
<th>2+</th>
<th>3-</th>
<th>3+</th>
<th>4-</th>
<th>4+</th>
<th>5-</th>
<th>5+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut-off Score</td>
<td>&lt;10</td>
<td>&lt;19</td>
<td>&lt;27</td>
<td>&lt;36</td>
<td>&lt;45</td>
<td>&lt;53</td>
<td>&lt;62</td>
<td>&lt;71</td>
<td>&lt;83</td>
<td>&lt;90</td>
</tr>
</tbody>
</table>

- Scores for a control requirement can range from 0 to 100
- A total score of 72 to 79 (a “3+”, or a solid “C” in academics) is considered the standard for a fully implemented control
- Scores over 80 generally indicate at least some aspect of the control requirements are monitored and/or managed to help ensure the control continues to remain fully implemented and effective
9. Breakdown by Control Areas

- This section provides a summary of the assessment results in terms of 19 topical control areas, which HITRUST refers to as CSF assessment domains
  - Facilitates the actual assessment process by grouping requirements that are typically handled by a specific office
  - Provides a more focused view on areas of particular interest to organizational leadership and external third parties
- The first page provides a histogram comparing assessment averages for each domain with the respective averages for all entities that have completed a validated assessment
- By reporting against standardized requirements, the organization can benchmark itself against other healthcare entities and help ensure it is providing an appropriate level of due care and due diligence for the protection of its information assets

- The remaining pages provide a table with a detailed summary of the assessor’s findings for each of the 19 CSF assessment domains
- The first column provides the CSF assessment domain that is addressed in the other two columns
- The second column provides the overall rating for the CSF assessment domain based on the 15-point maturity scale discussed earlier
- The third column provides the assessor’s comments for the CSF assessment domain
  - Summary of the assessor’s findings based on the evaluation of each CSF control requirement that maps to the CSF assessment domain
  - High-level recommendations on how the organization can achieve a higher rating for the CSF assessment domain, which can help improve implementation of the HITRUST CSF control requirements and further mitigate excessive residual risk to the organization’s information assets
App. A – Testing Summary

- HITRUST recognizes three (3) types of testing (or evaluation):
  - The review of applicable documentation, such as an organization’s written policies and procedures, organization charts, and network diagrams. It also includes the observation of processes or the implementation of certain controls, e.g., observing the amount of time it takes for a session to be automatically terminated or whether or not employees adhere to the organization’s clear/clean desk policy. This type of evaluation may also be referred to as “examination.”
  - Interviews with leadership, technical personnel, general users and other workforce members to identify actual practices (as opposed to written procedures) and gain other information relevant to the assessment
  - The conduct of technical testing, such as vulnerability scans, or the review of other independent testing such as that performed by an internal audit function or a third party professional services (PS) firm
- The appendix simply provides a laundry list of all the testing performed by the assessor organization
- HITRUST uses this information to help determine if testing could reasonably support the evaluation and scoring/rating of the controls required for CSF certification
- For more information on the HITRUST assessment methodology employed by an assessor organization, see https://hitrustalliance.net/documents/assurance/csf/CSFAssessmentMethodology.pdf
Appendix B – Corrective Action Plan

• This appendix provides two (2) tables that list the corrective actions needed to address the identified control gaps
  – Certification CAPs: identifies CAPs needed to meet the criteria for CSF
    • “3+” in all CSF Assessment Domains
    • “3+” for all controls; “3” plus CAPs or risk acceptance
  – Additional CAPs: Identified CAPs needed to ensure control requirements are fully implemented across the breadth and depth of the organization but do not adversely impact the criteria for CSF certification

For more information on CSF certification, see https://hitrustalliance.net/documents/assurance/csf/CSFAssuranceProgramRequirements.pdf

• Control Gap Identifier – The tracking number the organization assigns to the CAP entry to help distinguish one control gap (weakness or deficiency) from another
• Control Gap – The control gap that was identified and for which the organization needs to take action; this is expressed in the language of the CSF requirement that was assessed
• HITRUST CSF Control Mapping – The CSF control that contains/addresses the requirement that was found to have a gap (a weakness or deficiency) in its implementation
• Point of Contact (POC) – The individual or office that is responsible for addressing the control gap
• Scheduled Completion Date – The estimated date when all work associated with the corrective action will be finished and the CAP closed (marked completed) for the identified gap
• Corrective Actions – This is a brief description of the various actions or activities the organization will take to address the control gap; the actions are most often some form of remediation or “fix” but can be a formal acceptance of the excessive residual risk caused by the gap, if warranted.
• Status – Identifies whether the work has not yet been started, is ongoing, on hold, or completed
• Maturity Rating – This is the overall maturity rating computed for the control based on its assessment

For more information on risk and CAP prioritization, refer to https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf
Appendix C – Questionnaire Results

- **Title** – Provides the name of the organization subject to the assessment and the CSF version used.
- **Subtitle** – Provides the number and name of the CSF Assessment Domain for the controls that follow.
- **Related CSF Control** - Provides the number and name of the CSF control from which the HITRUST CSF Requirement Statement is derived.
- **HITRUST CSF Requirement Statement** – The CSF control requirement that was evaluated and the subject of the Maturity Assessment, Maturity Score, Maturity Rating, and Comments that follow.
- **Your Maturity Assessment** – The percentage of compliance with the requirements for each level of the maturity model: Policy, Process, Implemented, Measured and Managed.
- **Maturity Score** – The raw score for the requirement computed as the sum of the percentage of the points awarded for each maturity level (as indicated by the percentages contained in the maturity assessment above). Note the maximum points for each maturity level are: Policy – 25 pts, Process – 25 pts, Implemented – 25 pts, Measured – 15 pts, and Managed – 10 pts. In this example, the score was computed as (1)(25) + (1)(25) + (1)(25) + (.5)(15) + (.5)(10) = 87.5.
- **Maturity Rating** – The maturity rating of the control requirement derived from the maturity score. In this case, 87.5 falls between 87 and 90, which results in a 4+. (Refer to the table in the previous slide addressing Section 8.)
- **Comments** – A summary of the testing (evaluation) performed for the specified control requirement.

For more information on the maturity model and scoring approach, refer to [https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf](https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf)

- This appendix is generated from the MyCSF online assessment tool after the assessor submits the assessment for HITRUST validation and (possible) certification
- For more information on MyCSF, including downloadable brochures, refer to [https://hitrustalliance.net/mycsf/](https://hitrustalliance.net/mycsf/)
- For access to videos that describe various capabilities within MyCSF, refer to [https://hitrustalliance.net/mycsfvideos/](https://hitrustalliance.net/mycsfvideos/)
Appendix D – System Profile

- **System Name / ID** – The assessed organization’s name or identifier for the system
- **Group** – The business unit or similar functional element that owns the system (i.e., “system owner”)
- **Application** – What the system does, i.e., the business process or function the system provides
- **Hardware Platform** – The hardware on which the primary application is run. This may be as generic as “server” but some organizations provide more specific make and model information such as “Sun SPARC T5240”
- **O/S** – The underlying operating system that runs the system application, e.g., Windows 2010 or Unix. Note this could also be a specific hypervisor if the system application is run in a virtual container.
- **Database** – The database software that supports the system application. This may be as generic as “SQL Server” but some organizations provide additional information, such as “SQL Server 2014” or “Oracle 10g R2”
- **Location** – The physical location of the primary implementation or instantiation of the system. This may just include a city and state, but some organizations input more specific information such as “Primary Datacenter, Frisco, TX”
- **Prior Audit / Assessment** – The name and date of the last audit or assessment of the system, if applicable.
- **Description** – Additional information that describes the use of the system. Some organizations simply provide a generic descriptions such as “call center” or “client portal” similar to what is provided under “Application,” but some organizations provide more detailed information such as “The SYSTEM ID is the family of applications that supports BUSINESS UNIT 1 and BUSINESS UNIT 2.”

For more information on what should be included when scoping systems for an assessment, refer to https://hitrustalliance.net/documents/assurance/csfs/CSFAssessmentMethodology.pdf

- The System Profile List is developed by the HITRUST CSF Assessor in conjunction with the Assessed Entity
- The list includes all of the systems that were within the scope of the assessment
Section 3
HOW IT DESCRIBES AN ORGANIZATION’S SECURITY POSTURE
Multiple Requirements but One Information Protection Program

HITRUST provides a risk management framework (RMF) for the healthcare industry consistent with the NIST Cybersecurity Framework (CSF) and also addresses non-cyber threats:

- NIST CSF categorizes security controls according to an incident response process as opposed to the topical arrangement provided in a traditional RMF
- HITRUST CSF provides an integrated, harmonized set of requirements specific to healthcare as compared to individual references to controls in NIST and other frameworks
- HITRUST CSF Assurance Program provides a standardized evaluation and reporting approach fully supported by an integrated maturity model
- HITRUST CSF Assurance Program provides a pool of vetted assessor organizations and centralized quality assurance processes to ensure consistent and repeatable results

A Model for Healthcare Cybersecurity

- HIPAA Security, Data Breach Notification, & Privacy
- ISO 27799:2008
- CFR Part 11
- COBIT 4.1
- NIST SP 800-53 Revision 4
- NIST Cybersecurity Framework (CSF)
- NIST SP 800-66
- PCI DSS version 3.1
- FTC Red Flags Rule
- JCAHO IM
- 201 CMR 17.00 (State of Mass.)
- NRS 603A (State of Nev.)
- CSA Cloud Controls Matrix version 3.0.1
- CMS IS ARS version 2
- Texas Health and Safety Code (THSC) 181
- Title 1 Texas Administrative Code (TAC) 390.2
- MARS-E version 1
- IRS Pub 1075 (2014)

CSF Control Categories (Based on ISO 27001:2005)

- Information Security Management Program
- Access Control
- Human Resources Security
- Risk Management
- Security Policy
- Organization of Information Security
- Compliance
- Asset Management
- Physical and Environmental Security
- Communications and Operations Management
- Information Systems Acquisition, Development & Maintenance
- Information Security Incident Management
- Business Continuity Management
- Privacy Practices
The MyCSF Baseline Assessment

- Two major assessment types are available in the MyCSF GRC-based assessment management tool to support the HITRUST CSF Assurance Program
  - Baseline
    - Used to support HITRUST CSF Self-Assessment Reports, Validated Reports, and Certified Reports (“CSF Certification”)
    - Supports the generation of a partial compliance scorecard that minimally addresses each of the HIPAA Security Rule’s standards and implementation specifications
  - Comprehensive
    - Used as the basis for an organization’s entire information protection program
    - Provides the ability to assess 100% of the HITRUST CSF control requirements
    - Supports the generation of various scorecards, e.g., a complete compliance scorecard for the HIPAA Security Rule or a cyber readiness scorecard based on the NIST Cybersecurity Framework
- 2016 CSF v8 certification is based on a MyCSF baseline assessment
- A baseline assessment addresses 66 of 135 security-specific CSF controls (or 149 controls if privacy-specific controls are included), which are considered:
  - “High risk” based on the analysis of healthcare breach data and industry input
  - “High interest” based on the need to cover HIPAA Security Rule requirements
- Provides a reasonable level of assurance about the state of an assessed entity’s information protection program at a reasonable cost
- NIST specifically allows for the use of this type of approach to targeted assessments

“Organizations can use targeted risk assessments, in which the scope is narrowly defined, to produce answers to specific questions ... or to inform specific decisions[,] ... have maximum flexibility on how risk assessments are conducted, ... [and] are encouraged to use [NIST] guidance in a manner that most effectively and cost-effectively provides the information necessary to senior leaders/executives to facilitate informed decisions.”

(NIST SP 800-30 r1, p. 22)
HITRUST CSF Coverage of a MyCSF Baseline Assessment

- Focused on “high risk, high interest” control requirements
- Covers controls in 35 of 42 security-specific control objectives, indicated by (x/y) in the figure to the left
- For those control objectives not specifically covered:
  - 2.02 During On-boarding contains 1 control, 02.c Terms & Conditions of Employment, which is not assessed
  - 6.03 Information System Audit Consideration contains 2 controls, 06.i Information System Audit Controls and 06.j Protection of Information System Audit Tools; note auditing and monitoring is addressed in a baseline assessment in great detail via 09.10 Monitoring
  - 7.02 Information Classification contains 2 controls, 07.d Classification Guidelines and 07.e Information Labeling and Handling; note classification is a required element for 07.a, Inventory of Assets, which is addressed
  - 9.03 System Planning & Acceptance contains 1 control, 09.h Capacity Mgmt.; 09.05 Information Backup contains 1 control of the same name, the requirements for which are an integral component of 12.01 InfoSec Aspects of Bus. Continuity; 09.09 E-Commerce Services contains 3 related controls not assessed
  - 10.01 Security Req’s in Information Systems contains 1 control, 10.a Security Req’s Analysis & Specification, which is not assessed
- For the controls not specifically covered in the assessment regardless of control objective, the evaluation of 0.0 Information Security Mgmt. Program and 3.01 Risk Mgmt. Program will provide evidence of any gaps the organization has identified via internal and external assessments and audits, security incidents, data breaches and other sources, and whether or not the organization has taken corrective action
- Domain 13 Privacy Practices is not currently addressed
Assess Once and Report Many Times in Many Ways

• Cross-references allow granular scores at the requirement level to be “rolled up” in many and varied ways, both
  – Internal to the CSF, e.g., CSF control assessment domains (shown bottom right), CSF control objectives/categories (such as depicted below) and
  – External to the CSF, e.g., against the NIST CsF, HIPAA, AICPA Trust Services Principles & Criteria, PCI or SECURETexas (as seen to the right)

• No matter what the question about an entity’s information protection program, a CSF validated assessment can help provide the answers
Section 4

HOW YOU CAN ALIGN IT WITH YOUR CURRENT APPROACH
Actively Reading HITRUST CSF Validated and Certification Reports (1)

• **Step 1** – Confirm the organization name on the title page is correct or is an acceptable alternative (e.g., the Incorporated name versus the fictitious name). If not, request the organization provide the correct report.

• **Step 2** – Confirm the existence of (1) the Letter of Certification (or Validation, as appropriate) in Section 2 and (2) the Representation Letter from Management in Section 3. If either of these are missing, reject the report and request a complete/corrected copy of the report.

• **Step 3** – Review the assessment context in Section 4 and confirm (1) the name of the organization for which the report was prepared and (2) the date of the report match the name and date on the title page. If not, reject the report and request a corrected copy.

• **Step 4** – Make note of the organizational, regulatory and system risk factors identified in Section 4 and ensure these factors are appropriate to the intended scope of the assessment. For example, if the systems in scope contain credit card data, the Payment Card Industry Digital Security Standard (PCI DSS) should be included as one of the regulatory factors. If the factors do not adequately describe the scope of the assessment, determine what control gaps may exist and whether assurances around their implementation are needed. If needed, either request additional information from the assessed entity to address these gaps or reject the report and request a new one.

• **Step 5** – Review the scope of the assessment in Section 5 and determine if all the organizational business units, information systems, and outsourced services of interest, i.e., those for which assurances are required, are covered by the assessment. If not, determine what gaps may exist and request additional information to provide the necessary assurances. Alternatively, reject the report and request one with the required scope.

*Note that not all steps or the actions described in each step are necessarily sequential; e.g., concerns/issues identified in any one step may be addressed together after the complete review/reading of the report.*
Actively Reading HITRUST CSF Validated and Certification Reports (2)

- **Step 6** – Review the breadth and depth of the assessed organization’s information protection program in Section 6, including the types of technology deployed and the number and variety of independent assessments. Ensure level of program maturity is consistent with your expectations given the inherent risk the assessed organization presents. If not, review the findings for CSF Assessment Domain 1, Information Protection Program in Section 9 and determine if the scores and observations are consistent with your understanding of its maturity. Make note of the recommended actions for improving the overall maturity score for this domain and any CAPs that may exist for CSF controls 0.a, 03.a, 03.b and 03.c in Section 7 and Appendix B. Determine if the proposed corrective actions adequately address any concerns about the assessed organization’s information protection program, including any controls/requirements that are not specifically addressed by the assessment. Discuss any concerns you may have with the assessed organization and determine if additional corrective action will be taken or, if not, whether your organization is willing to accept any additional residual risk you perceive. (You may also wish to consider how the assessed organization compares to the rest of the industry via the benchmark information in Section 9.)

- **Step 7** – Review the remaining CSF Assessment Domains in Section 9. Verify the ratings match those in the benchmark diagram. If not, you may wish to request a corrected report. Ensure the ratings and the summaries for each CSF Assessment Domain adequately describe these areas. If not, review the findings for each relevant CSF control in Appendix C to determine if any perceived gaps in the Section 9 summaries are adequately addressed and/or consider requesting additional information from the assessed entity (based on the perceived level of excessive risk to your organization). Review the recommendations for improvement and, based on the domain score, compare the recommendations to the corrective actions identified in Appendix B and/or those for individual controls identified in Section 7 and Appendix C. If you believe there are gaps that have not been addressed to bring a CSF control requirement or CSF Assessment Domain score in line with certification requirements (generally a 3+ or a 3 with CAPs or formal acceptance of excessive residual risk), consider discussing the issue(s) with the assessed organization and obtain additional information/assurances as needed.
Actively Reading HITRUST CSF Validated and Certification Reports (3)

- **Step 8** – Review the results in Appendix C for any controls not reviewed in Steps 6 and 7, as needed, to address any particular concerns your organization may have regarding a specific requirement. For example, some organizations may have a particular interest in segmenting medical devices from the rest of the clinical network or restricting removable media to company-only devices. If these specific concerns are not adequately addressed by or documented in the report, consider requesting additional information/assurances from the assessed organization.

- **Step 9** – When conducting Steps 6 thru 8, you may wish to refer to Appendix A (as needed) to ensure testing adequately supports the assessment results documented in Sections 7 and 9 and in Appendix C. If not, consider discussing possible discrepancies with the assessed organization and obtain additional information/assurances.

- **Step 10** – Consistent with your overall third party assurance program requirements, formally document your “analysis” of the HITRUST CSF assessment report along with summaries of additional discussions, either internally or with the assessed organization, along with any recommendations and/or courses of action required.
Aligning Reports to Your Current Approach

- Relying organizations that already use the HITRUST CSF as the basis for their information protection program should have little difficulty in leveraging a HITRUST CSF assessment report to:
  - Provide assurances to internal stakeholders (e.g., executive leadership or internal audit) or external third parties (e.g., regulators).
  - Obtain assurances about a third party organization’s information protection program.

- However, organizations that do not already use or are otherwise unfamiliar with the HITRUST CSF may have difficulty relating the CSF controls to their own information security controls (safeguards), whether it’s based on another third party framework (e.g., PCI DSS) or it was built as a custom specification for the organization (e.g., based on the risk analysis process prescribed by NIST).

- You’ll need the HITRUST 2016 CSF v8 Standards and Regulations Cross-reference (xRef) (in Microsoft Excel format) and the CSF (in Adobe PDF format) to facilitate your work, copies of which are available in the CSF package downloadable from the HITRUST CSF License Agreement Webpage at https://hitrustalliance.net/csf-license-agreement/
More on the Documents You’ll Need

CSF PDF

• The CSF in Adobe PDF format provides a narrative description of all the control requirements, and is structured along the lines of ISO/IEC 27001:2005
  - 14 Control Categories
  - 45 Control Objectives parsed amongst the Categories
  - 149 Controls parsed amongst the Objectives
• Each control contains up to 3 implementation levels and may include 1 or more industry segments following the last level, which support
  - Special data requirements like card data and federal tax information
  - Special organizational requirements such as Health Information Exchanges
  - Other special requirements such as SECURETexas certification

HITRUST xRef Spreadsheet

• The xRef has multiple tabs, the first of which provides a cross-reference matrix from all the authoritative sources mapped to the HITRUST CSF at the control implementation level (see figure to the left)
• The remaining tabs provide mappings from individual authoritative sources to the HITRUST CSF at the control level (see figure to the right)
• Note mappings down to the individual MyCSF requirement statement (the level at which CSF assessments occur) are only available in the MyCSF assessment tool at this time
Mapping Your Controls to the HITRUST CSF

- If the controls you’ve specified for your information protection program are based on a framework like the Cloud Security Alliance’s Cloud Control Matrix (CSA CCM) or the Payment Card Industry Digital Security Standard (PCI DSS), the process of mapping your controls to the HITRUST CSF is generally straightforward.
- This will also work if you have proprietary controls based on a NIST-type risk analysis as long as you’ve already mapped them to one of the more comprehensive authoritative sources that are also mapped by HITRUST to the CSF (NIST SP 800-53 r4 being one of the best).
- Mappings can be done using a more high-level framework like AICPA’s Trust Services Principles and Criteria and even the NIST CsF, but it will require some work searching through the CSF for key terms, similar to the process described in the next example for proprietary programs.
- However, if you use a custom set of controls and you do not currently map them to a recognized standard like NIST, PCI DSS or CSA CCM, the mapping exercise will be more difficult and time-consuming.

Framework-based Program

- Determine if your framework controls have an authoritative source in common with the HITRUST CSF, e.g., NIST SP 800-53 r4.
- If not, consider mapping your controls to a common standard, such as NIST SP 800-53 r4.
- Cross-walk your controls to the CSF based on the common standard by:
  - Selecting a subset of controls or control requirements in the HITRUST CSF that have the same mapping to the control you wish to map, e.g., NIST AC-1.
  - Review the language in the subset of controls or control requirements and determine the best match.

Proprietary Program

- If you’ve mapped your controls to a common standard like NIST SP 800-53 r4, follow the directions for a framework-based program.
- If not, you’ll need to map your controls directly to the HITRUST CSF by:
  - Identifying the appropriate CSF Control Category for the proprietary control, e.g., 01. Access Control.
  - Selecting the CSF Control Objective for the proprietary control that fits best, e.g., 01.02 Access to Information Systems.
  - Reviewing the language in your control and identifying the CSF control that is the best match based on intent/content, e.g., 01.e Review of User Access Rights, or
  - If unable to determine a match, searching the CSF based on one or more key words or phrases.
Mapping a Framework-based Program to the CSF

Example – NIST-based Controls

• Assume your information protection requirements, including those for your third parties, are based on the controls contained in NIST SP 800-53 r4
• Assume your organization wants the events you’ve identified in your audit standard to reasonably support an investigation should a security incident occur

• You also know this requirement is derived from NIST SP 800-53 control AU-2 Audit Events, subparagraph (c), which states the organization:
  
  Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

• Referring to the “NIST SP 800-53” tab in the HITRUST CSF xRef spreadsheet, we see that AU-2 maps to the following CSF controls:
  - 09.aa Audit Logging
  - 09.ad Administrator and Operator Logs
  - 09.ae Fault Logging

• By looking up the CSF controls in the first tab of the xRef, “CSF Cross-Reference,” we note that AU-2 is mapped at levels 2, 1 and 1 for CSF controls 09.aa, 09.ad and 09.ae, respectively

• On inspection of the narrative for CSF control 09.aa, level 1 in the CSF PDF document, we find the relevant language:
  
  The organization shall provide a rationale for why the auditable events are deemed adequate to support after the fact investigations of security incidents and which events require auditing on a continuous basis in response to specific situations.

Example – PCI-based Controls

• Assume you’re interested in specific information protection requirements for a system that processes credit card information, and this regulatory requirement is within scope of the CSF assessment report you’re reviewing
• Subsequently you need to determine which CSF controls map to your controls that are tied directly to PCI DSS v3.1

• So let’s find where these requirements are located within the CSF by way of an example, such as the need to ensure the importance of cardholder data security is part of the security training & awareness program

• The requirement is derived from PCI DSS v3.1 control 12.6, which states the organization must:
  
  Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security

• Referring to the “PCI DSS v3.1” tab in the HITRUST CSF xRef spreadsheet, we see that 12.6 maps to the following CSF controls:
  - 02.e Information Security Awareness, Education & Training

• By looking up the CSF controls in the first tab of the xRef, “CSF Cross-Reference,” we note that 12.6 maps to 02.e level 2

• On inspection of the narrative for CSF control 02.e, level 2 in the CSF PDF document, we find the relevant language:
  
  The organization shall ensure the importance of cardholder data security is included in a formal security awareness program for all personnel.
Mapping a Proprietary Program to the CSF

• When organizations establish their own custom or proprietary controls, the number of controls and their specificity can vary significantly
• When the organization’s proprietary controls have been mapped to an industry-recognized or “best practice” control framework, the process of mapping them to their respective HITRUST CSF controls is relatively straightforward and can generally follow the same process for framework-based programs, which we outlined previously
• However, when the proprietary controls have not been mapped to such a control framework, the process becomes much more of a manual exercise, which may be performed by either (1) selecting a relevant CSF control category, objective and control to help narrow the search for an equivalent requirement, or (2) simply reviewing the results of one or more key word searches of the entire CSF

Example – Proprietary Controls

• Consider the following requirement: 
  Information containing sensitive information is not left in the open, unattended and unsecured.
• Although the requirement appears fairly specific, there are actually several issues that it could potentially cover; in addition to the typical “clear desk” or “clean desk” requirement, we might also wish to consider the security of documents left out on printers and facsimile machines as well as the security of portable media (assuming these other issues are not addressed elsewhere in your proprietary control framework)
• Clear/clean Desk – This is an access control requirement, CSF Control Category 1.0; is generally a user responsibility, which is addressed by CSF Control Objective 01.03; and appears to be addressed by CSF control 01.h Clear Desk and Clear Screen Policy
• The control specification for 01.h states, “A clear desk policy for papers and removable storage media and a clear screen policy for information assets shall be adopted,” which indicates the first and third of our concerns are addressed by the control
• By reviewing the 01.h level 1 control specification, it’s clear that the second of our concerns, the security of printers and facsimile machines, is also addressed
• Alternatively, one could search the CSF PDF on the following key terms to locate relevant control language: “clean desk” (0 matches), “desk” (29 matches), “clear desk” (6 matches), “printer” (4 matches), “facsimile” (8 matches), “fax” (7 matches), “portable media” (0 matches) and/or “removable media” (14 matches)
Section 5
WHERE YOU CAN FIND MORE INFORMATION
HITRUST Resources

Healthcare Sector CsF Implementation Guide
Discusses healthcare’s implementation of the NIST Cybersecurity Framework based on the HITRUST CSF and CSF Assurance Program

Risk vs. Compliance-based Protection
Discusses the difference between compliance and risk-based information protection programs and shows how controls are selected based on a risk analysis, after which their implementation becomes a compliance exercise

Risk Analysis Guide
Provides a detailed discussion of HITRUST’s NIST-based control implementation maturity model, HITRUST’s scoring model, and additional information on risk treatments, including remediation planning for control deficiencies

MyCSF vs. GRC Tools
Provides a discussion of the differences between a “typical” GRC tool and MyCSF, which was primarily designed to automate HITRUST’s assessment validation and certification process
https://hitrustalliance.net/documents/content/MyCSFVsGRCTool.pdf

CSF Assessment Methodology
Discusses HITRUST’s NIST-based approach to conducting CSF assessments, including information on how to determine organizational and system scope
https://hitrustalliance.net/documents/assurance/csfs/CSFAssessmentMethodology.pdf

CSF Assurance Program Requirements
Provides an overview of the CSDF Assurance Program, the various types of assessments available, and the process of obtaining and maintaining certification
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight