HITRUST® THIRD-PARTY ASSURANCE PROGRAM
Introduction to Third Party Assurance

Organizations rely upon a tremendous number of third-party vendors to handle everything from logistics to human resources, software development to financial recordkeeping, physical security to cybersecurity. Those third parties, especially those who have access to the organization’s network and sensitive data, represent an opportunity to improve services and lower costs. Each vendor also represents a potential risk to the security and privacy of information, which could present compliance risk. If a vendor is negligent or ill-prepared to protect the organization’s assets, the organization is impacted financially, reputationally and, many times, legally.

Organizations assess their vendors to understand privacy and security practices. Without that understanding, organizations cannot determine risk, and without determining risk, they cannot manage their risk effectively nor can they ensure compliance with regulations. It is also essential for vendors to be able to provide information and evidence about their privacy and security practices to their customers. Without this, the supply chain is at risk of a third-party breach that could, potentially, cripple their own organization.
Introduction to Third Party Assurance

The primary challenge in understanding and managing risk throughout this ecosystem is scale. Organizations have hundreds or even thousands of vendors; of different sizes, maturity and complexity. Similarly, vendors may have a small number of customers or possibly hundreds or thousands to serve. Effectively assessing the security posture up and down the supply chain is prohibitively expensive given the complexity of the risks presented by information privacy and system security concerns as well as an always-changing regulatory landscape both domestically and internationally.

It is also a huge challenge for organizations and their vendors to create, administer, respond to and manage assessments without a common understanding of security and privacy best practices. Due to complexity in the regulatory landscape, HITRUST has studied the requirements to build a single security framework from which they could be assessed once, and by which they could report many. Keeping it up to date while providing the tools for organizations of any size to administer those assessments and effectively manage third-party risk.

With HITRUST, organizations can manage and interpret the results using a vetted, standardized, assurance process for reporting. Therefore, providing assurances around the assessed organization’s security posture. The framework also includes services to offload the administrative burden and streamline the electronic exchange of assessment information.
Section 1

Drivers and Challenges... Third Party Assurance
What's Driving Demand for Increased Assurance?

1. Increasing risk posed by third parties
2. Increasing cyber threat landscape
3. Confusion
   - What is reasonable, appropriate or adequate?
4. Growing compliance risk and liability
   - Breach and legal costs; regulatory penalties; impact to brand and reputation
What are Customer Challenges to Implementing and Executing a Third Party Assurance Program?

Customers face many challenges in effectively measuring and managing risk relating to their vendors, including:

- Complexity of contracting process due to organization-specific security requirements
- Difficulty tracking down appropriate contacts at business partners
- Low rate, inaccurate and incomplete responses to assurance requests
- Inadequate due diligence of questionnaires or assessment requests
- Difficulty monitoring the status and effectiveness of corrective action plans
- Costly and time-intensive data collection, assessment and reporting processes
- Inability to proactively identify and track risk exposures at business partner
- Lack of visibility into downstream risks related to business partners (i.e., business partners' own vendors)
- Lack of consistent reporting to management on business partner risks
What are Business Partner Challenges With Third Party Assurance?

Business partners face many challenges in effectively responding to and meeting assessment and assurance requests from customers, including:

• Complex contracting process due to unique security requirements
• Wide variety of questionnaires and assessment requests - inability to effectively leverage responses across customers
• Varied expectations around corrective action plans
• Expensive and time-intensive audits by customers
• Inability to consistently report to and communicate with customers
HITRUST has been working with customers and business partners to identify a practical and implementable approach.

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 vendor to communicate their information privacy and security posture (relating to the same scope of services).

Nor does it make sense to maintain and support organization-specific assessment methodologies and multiple assessments for each organization.

HITRUST has been working with customers and business partners to identify a practical and implementable approach.
Section 2
Key Elements of the Approach
Key Elements of the Approach

Reliability is obtained through the five key elements of the approach

- Transparency
- Accuracy
- Consistency
- Scalability
- Efficiency

HITRUST CSF® Assurance Program

- Utilizes a common set of information security requirements with standardized assessment and reporting processes
  - Improved efficiency & lowered costs
- The oversight and governance provided by HITRUST supports a process whereby organizations can trust that their third parties have essential security and privacy controls in place and can understand their effectiveness
- [https://hitrustalliance.net/csf-assurance/](https://hitrustalliance.net/csf-assurance/)
Key Elements of the Approach

**Transparency** - The approach should be open and transparent.

Requirements are agnostic for similar types of sensitive information

- Integrates relevant federal control baselines; incorporates industry leading practices; leverages threat-to-control relationships; incorporates risks based on past breach data and the current threat environment

The entire program is publicly available and commonly understandable

- Control framework/requirements; assessment methodology/procedures; scoring model

**Accuracy** - The approach should ensure accuracy in evaluation and reporting of the implemented controls

HITRUST uses a 5x5 control maturity and scoring model to evaluate the HITRUST CSF’s control requirements

- 5 maturity levels for each control requirement;
- 5 scoring levels for each control maturity level

HITRUST also provides a scoring rubric for each maturity level
Key Elements of the Approach

Consistency - The approach should ensure consistency in evaluation and reporting regardless of the specific assessor used.

Extensive assessment guidance
• General guidance for each maturity level
• Specific guidance for each control

HITRUST quality assurance review process
• Applies to all third-party assessments

Standardized reporting format
Key Elements of the Approach

**Scalability** - The approach should be scalable enough to address the needs of the entire industry, while maintaining consistency and accuracy.

**Formal HITRUST CSF® Assessor Program**
- HITRUST CSF trained and authorized assessors
- Experience/capabilities vetted by HITRUST

Choose from a pool of authorized HITRUST CSF Assessors to ensure
- The best fit and price

**Program is market-based**
- As demand for assurance increase, so does the pool of HITRUST CSF Assessor organizations
Key Elements of the Approach

**Efficiency** - The approach should allow an organization to assess once then report many, i.e., an assessment must address multiple compliance and best practice requirements and support the reporting of assurances tailored to each requirement.

HITRUST fully leverages the ‘Assess Once, Report Many’ approach

- Multiple security requirements (e.g., legal, regulatory)
- One cybersecurity program
- One targeted, cost-effective assessment that provides a reasonable level of assurance at a reasonable cost
- Multiple reporting options from a single assessment
Key Elements of the Approach

**Reliability** - The approach should provide a high degree of assurance for relying parties, such as internal stakeholders (e.g., customers, business partners, vendors and regulators.)

**Obtained Through:**
- Transparency
- Accuracy
- Consistency
- Scalability
- Efficiency

**Provided By:**
- HITRUST CSF
- HITRUST CSF Assurance Program
- HITRUST CSF Assessors Program
- HITRUST CSF Assurance Program
HITRUST CSF Based Reporting Options

The HITRUST CSF Assurance program supports efficiency of assessment by allowing one assessment to be used to create numerous reporting options, reduce costs and save resources

<table>
<thead>
<tr>
<th>Consideration</th>
<th>HITRUST CSF Report</th>
<th>SOC 2 Report with HITRUST CSF</th>
<th>SOC 2 + HITRUST CSF Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of report (Relevant Standard)</td>
<td>HITRUST CSF Assurance</td>
<td>AT101</td>
<td>AT101 + HITRUST CSF Assurance</td>
</tr>
<tr>
<td>Scope of report</td>
<td>HITRUST CSF controls (requirements may or may not be limited to those required for certification)</td>
<td>Security, availability, and confidentiality Trust Services Principles; HITRUST CSF controls (may or may not be limited to those required for certification)</td>
<td>Security, availability, and confidentiality Trust Services Criteria; HITRUST CSF controls (requirements may or may not be limited to those required for certification)</td>
</tr>
<tr>
<td>Intended Users</td>
<td>Unlimited distribution</td>
<td>Limited distribution</td>
<td>Mixed distribution (Limited/ Unlimited)</td>
</tr>
<tr>
<td>Resulting Deliverable</td>
<td>HITRUST CSF report with background, mgmt. rep., scope, results of maturity scores, CAPs, <strong>NIST CsF scorecard/certification</strong></td>
<td>Attest Opinion with description of systems &amp; service auditor test/ results against selected Trust Services Principles; HITRUST CSF controls (suitable criteria)</td>
<td>Attest Opinion with description of systems &amp; service auditor test/ results against selected Trust Services Principles, HITRUST CSF controls (suitable criteria); HITRUST CSF report with background, mgmt. rep., scope, scores, CAPs, <strong>NIST CsF scorecard/certification</strong></td>
</tr>
<tr>
<td>Report issued by</td>
<td>HITRUST</td>
<td>Independent CPA firms</td>
<td>Independent CPA firms, HITRUST</td>
</tr>
<tr>
<td>Report Addresses</td>
<td>HITRUST CSF, NIST CsF</td>
<td>HITRUST CSF, AICPA Trust Services Criteria</td>
<td>HITRUST CSF, AICPA Trust Services Criteria, NIST CsF</td>
</tr>
</tbody>
</table>
Attributes of a Good Risk Management Framework

• The framework should provide **comprehensive coverage** of general security requirements and provide **prescriptive controls** (safeguards), i.e., the control requirements should be detailed support implementation in the intended environment and adequately address the threat(s).

• The framework’s controls should be **practical** for an organization to implement and maintain, and **scalable** based on the size and type of organization or information system being protected.

• The controls and implementation, assessment and reporting methodologies should be vetted by organizations and industry experts such as leading professional services firms via an open and **transparent** development and update process.

• The controls specified in the framework should be supported by detailed audit or assessment guidance that helps ensure **consistency** and **accuracy** in evaluation and reporting regardless of the specified assessor used.

• The framework should be **efficient** and allow an organization to ‘assess once and report many’, i.e., an assessment must address multiple compliance and best practice requirements and support the reporting of assurances tailored to each requirement.

• Evaluation of the framework’s implementation should be **reliable**, i.e., organizations should be able to rely on the assurances provided by internal and external assessments.
Section 3
Third-Party Assurance (TPA) Risk Triage Methodology
What exactly is risk triage and why would I want to use it?

• Risk triage in this context is an abbreviated approach to assessing a third-party's (supplier's) overall security risk without investing the resources required to perform a traditional in-depth risk assessment
  – Categorizes third-parties by the level of risk they present to the organization
  – Identifies an assurance mechanism most appropriate to the category of risk
• Risk triage allows organizations to
  – Focus assurance efforts on third parties/suppliers that present the most risk
  – Increase efficiency and reduce costs while managing third-party/supply chain risk within organizational risk tolerances
How does risk triage fit in an organization’s third-party risk management program?

- Manage third-party/supplier risk
  - By qualifying third parties/suppliers
    - Based on the inherent risk they represent
      - Via an appropriate assurance mechanism
Can you explain how the HITRUST risk triage methodology works?

<table>
<thead>
<tr>
<th>Risk Component</th>
<th>Risk Factor Type</th>
<th>Risk Factor</th>
<th>Risk Factor Rating</th>
<th>Risk Factor Type Score</th>
<th>Risk Comp. Score</th>
<th>Risk Score</th>
<th>Assessment Type (Based on Risk Score)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact (I)</td>
<td>Organizational (O)</td>
<td>IO1: Percentage of organizational data</td>
<td>0 – 4</td>
<td>Simple Average 0 – 4</td>
<td>High Watermark 0 – 4</td>
<td>0 – Facilitated or Remote Self-Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IO2: Total amount of organizational data</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td>1 – Validated Assessment w/ CAPs; No Minimum Score</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IO3: Criticality of the business relationship</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td>2 – Validated or Certified Assessment; Consolidated Score &gt; 62 w/ CAPs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance (C)</td>
<td>IC1: Comprehensive and specificity of requirements</td>
<td>0 – 4</td>
<td>Simple Average 0 – 4</td>
<td></td>
<td>3 – Validated or Certified Assessment; Consolidated Score &gt; 71 w/o CAPs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IC2: Level of assurance required</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td>4 – Validated or Certified Assessment; Consolidated Score &gt; 87 w/ or w/o CAPs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IC3: Specified or observed fines and penalties</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IC4: Level of enforcement</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likelihood (L)</td>
<td>Technical (T)</td>
<td>LT1: Data processing environment</td>
<td>0 – 4</td>
<td>Simple Average 0 – 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LT2: Type of cloud environment, if used</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LT3: Data access approach</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LT4: Data storage location</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LT5: Use of subcontractors</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why is the HITRUST Risk Triage Methodology better than other approaches?

- Simple, open model
- Based on inherent risk of the relationship
- Leverages the HITRUST CSF®
  - Demonstrates appropriate level of due diligence
- Leverages the HITRUST CSF Assurance Program
  - Demonstrates appropriate due care
- Transfers costs to third parties/suppliers
  - Reduces need/scope of internal resources
- Reduces costs for third parties/suppliers
  - “assess once, report many”
- Provides three dimensions of assurance (trust)
Section 4
Facilitating Administrative Functions and Electronic Exchange of Assessment Information
The HITRUST Assessment XChange™

The HITRUST Assessment XChange streamlines and simplifies the process of managing and maintaining risk assessment information from your third parties or vendors by:

- Offloading the administrative and time-consuming activities, including identifying the appropriate individual or function at a third-party, including assurance requirements and receiving status information
- Delivering a HITRUST CSF Assessment report in a format that can be consumed for review, analysis and input into existing third-party risk management systems
- Reduces the need for third parties to respond to multiple customer inquiries
How Does the Assessment XChange Help?

Third-party outreach
• Contacts third parties, and identifies points of contact
• Coordinates third-party assessment management and tracking ensures efficient outreach and emphasizes importance
• Coordinated outreach on behalf of multiple organizations

Third-Party education
• Experienced HITRUST personnel to explain and answer questions on the assessment & assurance processes

Third-party assessment expectations
• Ensuring that the assessment information obtained from third parties is inline with customer contractual obligations

Visibility into status of third parties/third-party assurance
• Provides status updates during the process to support progress tracking
• More granular information about a third party’s security posture including CAPs and GAPS by providing the full report

Provides the ability to electronically receive or export results in a format that is easy to consume into GRC or VRM solutions
• Open API integration to existing vendor risk management and governance risk and compliance tools
• Create and report on security metrics across a third-party population
Why Participate in the Assessment XChange?

**Improved vendor compliance**
- Leverages multiple requests and established relationships with third parties across the HITRUST Assurance program

**Improved ROI**
- More cost effective by shifting assessment costs to the third parties
- Offloads the administrative and time consuming activities

**Improved third-party risk management**
- Provide the ability to electronically receive or export results in a format that is easy to consume into vendor risk management solutions enabling automated vendor monitoring
- Allows internal resources to better spend time on more targeted residual risk to the organization
Summary of the HITRUST Third Party Assurance Program

The HITRUST Third Party Assurance program brings together key HITRUST programs such as the HITRUST CSF, HITRUST CSF Assurance, CSF Assessors and HITRUST Assessment XChange to provide substantial benefits to organizations relating to third-party risk including:

01
• Increased efficiencies and timeliness
  • Improved vendor relations

02
• Reduced Information Risk
  • Reduced Costs associated
Section 6
Provider TPRM
Provider TPRM

Prominent Chief Information Security Officers (CISOs) from leading health systems and providers throughout the country have come together to establish the Provider Third-Party Risk Management Council to develop, recommend and promote a series of practices to effectively manage their information security-related risks in their supply chain and to safeguard patient safety and information.

Why is this important?

Effectively assessing the security posture up and down the supply chain is prohibitively expensive given the complexity of the risks posed by information privacy and system security concerns as well as an ever-changing regulatory landscape both domestically and internationally. The challenges they face go well beyond their resources and capabilities, posing a huge challenge for organizations and third parties to create, administer, respond to and manage assessments. In addition, ineffective security, compliance and assurance methods drive cost and confusion within organizations and across third parties.

Learn more: Provider-TPRM.org
Section 7

Common Questions
I thought the HITRUST CSF was for Healthcare?

- The HITRUST CSF provides coverage across multiple regulations and includes significant components from other well-respected IT security standards bodies and governance sources.
- It is scalable, risk based, industry agnostic and certifiable

### Legislative, Regulatory, and "Best Practice" Standards and Frameworks include, but are not limited to:

- COBIT 4.1
- NIST SP 800-53 Revision 4
- NIST Cybersecurity Framework (CSF)
- DHS Cyber Resilience Review
- PCI DSS version 3
- FTC Red Flags Rule
- FFIEC IT InfoSec Examination
- 201 CMR 17.00 (State of Mass.)
- NRS 603A (State of Nev.)
- CSA Cloud Controls Matrix version 3.1
- CIS CSC version 6 (SANS Top 20)
- CMS IS ARS version 2
- MARS-E version 2
- IRS Pub 1075 v2014
- FedRAMP, NY & GDPR

### Control Categories

0. Information Security Management Program
1. Access Control
2. Human Resources Security
3. Risk Management
4. Security Policy
5. Organization of Information Security
6. Compliance
7. Asset Management
8. Physical and Environmental Security
9. Communications and Operations Management
10. Information Systems Acquisition, Development & Maintenance
11. Information Security Incident Management
13. Privacy Practices

### Scoping Factors

**Regulatory**
- Federal, state and domain specific compliance requirements

**Organization**
- Geographic factors
- Number of records processed or held

**System**
- Data stores
- External connections
- Number of users/transactions
Does This Mean I Have to Redo My Security Program?

The HITRUST CSF covers 100% of the:

- ISO 27002-2005 controls (mapping is trivial, as the HITRUST CSF is built on ISO 27001-2005)
- ISO 27002-2013 controls (depicted on the left)
- NIST SP 800-53 r4 controls, moderate-level baseline (depicted on the left)

To simplify the process of aligning from a standard like ISO or NIST to the HITRUST CSF, HITRUST provides a *HITRUST CSF Standards & Regulations Cross-Reference (X-Ref)* spreadsheet with detailed mappings (depicted by the examples on the right)

*HITRUST CSF control category 0.0 addresses the original ISMS requirements in Section 4 of ISO 27001:2005*
Does a HITRUST CSF Assessment Comply With HIPAA’s Risk Analysis Requirements?

- HITRUST provides the most prescriptive, yet flexible, controls-based risk management framework in the industry
- Thousands of HITRUST CSF assessments have been conducted by and for public and private sector organizations since 2009
- HITRUST CSF assessments have been used successfully by many organizations to address OCR audits and in support resolution agreements
- In fact, HHS specifically references HITRUST’s approach in its *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*

The HIPAA Security Rule requires organizations to “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information… [and] implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.” [HIPAA § 164.308(a)(1)(ii)(A)-(B)]

By selecting and tailoring the NIST SP 800-53 moderate baseline through specification of control parameters and the integration and harmonization of multiple, industry-relevant standards and best practice frameworks, HITRUST leverages the underlying risk analysis used to create the NIST SP 800-53 security controls catalog to provide an industry-level control overlay, as described by NIST.
How Does All This Facilitate Trust?

Targeted Organizations/ Business Associates

- Self-Assessment
- Validated Assessment

MyCSF Security / Comprehensive Assessment

- Entity completes Assessment
  - Lower Degree of Testing
    - CSF Self-Assessment Report
  - Higher Degree of Testing
    - HITRUST Quality Control
    - CSF Validated Report
    - CSF Validated Report with Certification
What are the Advantages of a HITRUST CSF Assessment Report over a SOC 2 Report?

- **Transparency**
  - Prescriptive control requirements versus organization-designated controls
- **Consistency**
  - Reports issued by HITRUST versus assessors/CPA firms
- **Accuracy**
  - Certification determined by HITRUST based upon quantitative and qualitative factors
- **Reliability**
  - Additional level of quality assurance and review procedures performed by HITRUST
What are the Benefits of Combining HITRUST CSF Assessments & SOC 2 Reporting?

• Leverage the HITRUST CSF controls in SOC 2 engagements
• Realize significant time efficiencies and cost savings by synergies between the HITRUST CSF controls and Trust Services Criteria
• Reduce the inefficiencies and costs associated with multiple reporting requirements
• Increase transparency and communicate to stakeholders through a single deliverable
• Consider service organizations’ controls both from the SOC 2 criteria and HITRUST CSF criteria
Does the HITRUST CSF meet the Definition of Suitable Criteria for SOC 2 Reporting as Defined by the AICPA?

Yes. The practitioner must have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users. Criteria are the standards or benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. Suitable criteria must have each of the following attributes:

- **Objectivity**—Criteria are free from bias.
- **Measurability**—Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- **Completeness**—Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users made on the basis of that subject matter.
- **Relevance**—Criteria are relevant to the subject matter.

Criteria that are established or developed by groups composed of experts that follow due process procedures, including exposure of the proposed criteria for public comment, are ordinarily considered suitable. The HITRUST CSF has been developed by HITRUST in collaboration with security professionals following due process that includes a comment process and therefore meets the requirements for suitable criteria. Because the criteria are made available to the users of the report in the SOC 2 + HITRUST CSF report, they also meet the requirement for available criteria.

*For more information & additional resources, visit [https://hitrustalliance.net/soc2/](https://hitrustalliance.net/soc2/)*
Why Can’t I Just Use the NIST Cybersecurity Framework?

The HITRUST CSF provides the foundation needed to implement the NIST Cybersecurity Framework.

Although scalable, the NIST CSF lacks prescription in:

- Requirements
- Assessment methodology

Subsequently lacks:

- Transparency
- Accuracy
- Consistency
- Efficiency
- Reliability
Why Can’t I Just Do the AICPA Cyber Examination?

AICPA Cyber Examination consists of two major components:
• A description of an entity’s program based on new description criteria
• An assessment of control effectiveness based on its control criteria

As with the AICPA Trust Services Principles, additional information (specificity) is needed to address the criteria, and the Cyber Examination would result in a reduction of the following when viewed across multiple entities:
• Transparency
• Accuracy
• Consistency
• Reliability
How Do I Know What Was in Place and Tested?

HITRUST CSF Validated and Certified Report

- Letter of Certification
- Representation Letter
- Assessment Context
- Assessment Scope
- Security Program Analysis
- Assessment Results
- Overall Security Program Summary
- Breakdown of Controls Required for Certification
- Testing Summary
- Corrective Action Plan
- Questionnaire Results (Detailed)
- System Profile
How Do I Benefit From All This?

- Redundant, inconsistent assessments result in lost productivity, additional costs
- A more efficient, streamlined approach benefits the customer and vendor
- Recommended approach leverages:
  - A single controls framework for context
  - A strong assessment methodology that provides high assurance and consistency
  - A single assessment to provide efficient reporting
    - **HITRUST CSF** – control maturity scoring
    - **SOC 2** – HITRUST CSF provides SOC 2 the necessary prescriptiveness and transparency for availability, confidentiality and security criteria
    - **NIST Cybersecurity Framework** – HITRUST CSF provides basis for consistency, HITRUST CSF Assurance enables transparency and assurance, and scorecard enables reporting on NIST CsF Core Subcategories
What if we need an information privacy and security assessment before an organization can complete their CSF Validated Assessment or Certification?

This can be accomplished by utilizing a HITRUST Self-Assessment which is used in place of your current questionnaire. This allows vendors to provide assurance information quickly and takes them down the path of utilizing a standardized assessment approach.

The self-assessment leverages the CSF Assurance program allowing the vendor to then have a third party validate the assessment information to obtain a CSF Validated Assessment without having to reenter the assessment information or understand another approach.
Because our organization is adopting the HITRUST Third-Party Assurance program, does this mean we have to become HITRUST Certified?

No, your organization does not have to become HITRUST Certified or undergo a HITRUST CSF Assessment.

However, we strongly suggest your organization does undergo a HITRUST CSF Assessment to better understand your own security posture.
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.

https://hitrustalliance.net/documents/cs3_rmf_related/RiskVsComplianceWhitepaper.pdf

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.


HITRUST MyCSF® vs. GRC Tools

Provides a discussion of the differences between a "typical" GRC tool and HITRUST MyCSF, which was primarily designed to automate HITRUST’s assessment validation and certification process.

https://hitrustalliance.net/documents/content/MyCSF_VsGRCTool.pdf

Risk Management Frameworks Whitepaper

How HITRUST provides an efficient and effective approach to the selection, implementation, assessment and reporting of information security and privacy controls.

https://hitrustalliance.net/documents/campaigns/HITRUST-RMF-Whitepaper-FM.pdf

CSF Assurance Program Requirements

Provides an overview of the CSF Assurance Program, the various types of assessments available, and the process of obtaining and maintaining certification.

HITRUST Blog Resources

For more resources, visit our HITRUST Blog
HITRUST 2019 Snapshot

Background
1) Founded in 2007
2) HITRUST Alliance, Inc. is a non-profit responsible for frameworks, standards and methodologies
3) HITRUST Service Corporation is a for-profit responsible for training and tools

Adoption
1) HITRUST CSF is utilized by 81% of U.S. hospitals and health systems and 83% of U.S. health plans
2) HITRUST CSF is the most widely adopted control framework in the healthcare industry, according to a 2018 HIMSS survey
3) HITRUST CSF Assurance program is the most widely adopted program for assessing third party risk

Best Known for
1) Developing the HITRUST CSF – 9th major release
   - Development guided by a CSF Advisory Council comprised of AHA, AMA, AHIP, AGMA and other security/privacy experts
   - Basis for the health and public sector implementation guidance for the NIST Cybersecurity framework, recognized by Department of Homeland Security (link) and Department of Health and Human Services (link)
   - Deemed an acceptable controls by the AICPA for a SOC 2 examination
   - Identified as an appropriate standard to safeguard Internet of Things (IoT) by NIST (link)
2) Operating the healthcare industry’s Information Sharing and Analysis Organization (ISAO)
For more information on HITRUST's Programs visit www.HITRUSTAlliance.net

To view our latest documents, visit the Content Spotlight