Agenda

Introduction to Third-Party Assurance: Drivers and Challenges

Key Elements of an Effective Assurance Program

Implementing the HITRUST Third-Party Assurance Program

HITRUST Assessment XChange: Improving Efficiency and Effectiveness

Provider Third-Party Risk Management (PTPRM)
Introduction to Third-Party Assurance

Challenge
Organizations rely upon third-party vendors for a wide range of services
• Third-party access to data represents a potential risk
• When a third party is unable to protect the data, the organization is impacted (financially, reputationally, legally)

Organizations must assess vendors to:
Understand privacy and security practices ➔ determine risk ➔ manage risk effectively & comply with regulations

The process to understand and manage risk is difficult due to scale and complexity

Solution
HITRUST built a framework, assurance program, and assessor program to bring not just assess once, report many but also transparency, consistency, scalability and reliability.
Section 1
Drivers and Challenges... Third-Party Assurance
What is Driving Demand for Increased Assurance?

1. Increasing risk posed by third parties
   Growing number of third parties with access to sensitive data

2. Changes in landscape
   Increasing cyber threats

3. Confusion
   What is reasonable, appropriate or adequate?

4. Growing compliance risk and liability
   Breach and legal costs; regulatory penalties; impact to reputation
Customer Challenges to Managing Third-Party Risk

- Complexity of contracting
- Appropriate contacts
- Inaccurate and incomplete responses
- Due diligence of questionnaires
- Monitoring status and effectiveness
- Time-intensive process
- Proactively identifying and tracking risk exposures
- Visibility into downstream risks
- Consistent reporting to management
Business Partner Challenges

- Complexity of contracting
- Variety of questionnaires
- Expectations around corrective action plans
- Time-intensive audits
- Consistent reporting to customers
For a vendor to communicate their information privacy and security posture,

There are no scenarios where performing 15, 50 or 250+ unique assessments makes sense

• Proprietary questionnaires
• Time-consuming
• Adds costs to the system

HITRUST has been working with organizations and third-party vendors to identify a practical and implementable approach.
Section 2
Key Elements of An Effective Assurance Program
Attributes of a Good Risk Management Framework

• Provides **comprehensive coverage** of general security requirements and **prescriptive controls** (safeguards)
• Is **efficient** and allows an organization to ‘assess once and report many’
• Has an implementation that is **reliable**, i.e., organizations should be able to rely on the assurances provided by internal and external assessments
• Follows a risk-based approach offering **multiple levels of implementation requirements** determined by specific risk thresholds
• Has controls that are:
  – **Scalable** based on the size and type of the organization or information system being protected
  – **Practical** to implement and maintain
  – Supported by detailed audit or assessment guidance that helps ensure **consistency** and **accuracy** in evaluation and reporting regardless of the specified assessor used
• 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
**Reliability.** The assessment approach should provide a high degree of assurance for relying parties including customers, business partners, vendors and regulators.
Launching an Effective Third-Party Assurance Program

1) Start with the right risk management framework
2) Ensure reliability through the right methodology

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

Provided By:
- HITRUST CSF
- HITRUST CSF Assurance Program
- HITRUST CSF Assurance Program
- HITRUST CSF Assessor Program
- HITRUST CSF Assurance Program
Five Key Elements to Achieving Reliability

HITRUST CSF Assurance Program

• A common set of requirements
• Standardized assessment and reporting processes
• Improved efficiency and lower cost
• Third parties have essential controls in place
• Control effectiveness is well understood

https://hitrustalliance.net/csf-assurance/
Key Elements of The Approach

**Transparency**
- Consistent for similar types of sensitive information
- Relevant federal control baselines
- Threat-to-control relationships
- Past breach data
- Current threat environment

The entire program (framework, methodology, scoring) is publicly available and commonly understandable

**Accuracy**
- 5x5 control maturity and scoring model
- 5 maturity levels for each control requirement
- 5 scoring levels for each control maturity level
- Scoring rubric for each maturity level

**Consistency**
- General guidance for each maturity level
- Specific guidance for each control

- Quality assurance review process applies to all third-party assessments
- Standardized reporting format
Key Elements of The Approach

**Scalability**
- Assessors trained, authorized, and vetted by HITRUST
- Pool of HITRUST CSF® Assessor organizations scales with market demand
- Choices ensure best fit and price

**Efficiency**
- Assess once, report many
- Legal, regulatory requirements
- Single cybersecurity program
- Reasonable assurance at reasonable cost
- Multiple reporting options (e.g. NIST CSF, SOC II)
The Value of a HITRUST CSF Assessment

- Forward looking
- Transparent
- Quantified control maturity
- Satisfies all other common TPA reporting standards
- Three levels of validation provide consistency, limit subjectivity
- Could eliminate current proprietary questionnaires

Assess Once, Report Many™
Section 3
Implementing the HITRUST Third-Party Assurance Program
What is the TPRM Qualification Process and Why Use it?

- Part of the HITRUST TPRM Methodology
- Quickly estimates overall security risk without investing the resources required to perform a traditional in-depth risk assessment
  - Categorizes third parties by the level of inherent risk they present to the organization
  - Identifies an assurance mechanism most appropriate to the category of risk
- Formal (re)qualification 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
What Does the TPRM Qualification Process Provide?

- Information needed to help organizations triage third parties based on inherent risk
- A standardized risk triage approach based on specific inherent risk factors
- Recommendations for an appropriate assurance mechanism based on inherent risk
- A reiterative process for achieving a requisite level of assurance
- Formal acceptance based on risk targets (target profile) and residual risk (current profile)
## How Does Risk Triage Identify an Appropriate Assessment?

<table>
<thead>
<tr>
<th>Risk Component</th>
<th>Risk Factor Type</th>
<th>Risk Factor</th>
<th>Risk Factor Rating</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></td>
<td>0 – Facilitated or Remote Self-Assessment</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>
</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>
</tr>
<tr>
<td></td>
<td>Compliance (C)</td>
<td>IC1: Comprehensiveness and specificity of requirements</td>
<td>0 – 4</td>
<td>High Watermark 0 – 4</td>
<td>Simple Average (Rounded UP to the Next Highest Integer) 0 – 4</td>
<td>3 – Validated or Certified Assessment; Consolidated Score &gt; 71 w/o CAPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IC2: Level of assurance required</td>
<td>0 – 4</td>
<td></td>
<td>Simple Average 0 – 4</td>
<td>4 – Validated or Certified Assessment; Consolidated Score &gt; 87 w/ or w/o CAPs</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>
</tr>
<tr>
<td></td>
<td></td>
<td>IC4: Level of enforcement</td>
<td>0 – 4</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>
</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>
</tr>
<tr>
<td></td>
<td></td>
<td>LT3: Data access approach</td>
<td>0 – 4</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>
</tr>
<tr>
<td></td>
<td></td>
<td>LT5: Use of subcontractors</td>
<td>0 – 4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why is HITRUST TPRM Qualification 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)

Level of Protection
(CSF Control Specification)

Level of Assessment
(Self or Independent)

Level of Control Implementation
(CSF Control Maturity)
Section 4
Accelerate Administrative Functions and Simplify the Exchange of Assessment Information
Operationalizing Assessment Requirements

What do you need to do to acquire assessments from third parties?
1. Handle internal and external negotiations
2. Appropriate contractual language
3. Notify third parties
4. Determine assessment due dates and timelines
5. Make informed management decisions and respond to special conditions
6. Monitor status
7. Receive and review assessments

The current process is time-intensive to implement and manage.
Solution = HITRUST Assessment XChange™
A Partner for Your Third-Party Risk Management Program

The HITRUST Assessment XChange is an innovative solution designed to streamline and simplify third-party risk management.

We are the leaders in providing organizations with the methodologies, tools and services needed to efficiently and effectively qualify third parties for potential business relationships with a common approach that can be used across industries for all third-party risk management.
What Makes the HITRUST Assessment XChange Unique?

The HITRUST Assessment XChange has three proprietary key elements:

1. **Methodology**
   The foundation of the XChange is our Third-Party Risk Management Qualification Methodology – a groundbreaking approach for organizations to minimize risk from third-party relationships – established by HITRUST®, the global leader in information risk management and compliance.

2. **Expert Support Team**
   The XChange is driven by a team of Onboarding Support Specialists – experts dedicated to ensuring a positive experience for your third parties, as well as transparent and comprehensive results for your organization.

3. **Innovative Exchange Platform**
   Powering everything is the user-friendly XChange Manager SaaS tool. This secure portal serves as a platform to automate communications and report delivery. Everything you do today, in one convenient location.

The XChange is a turnkey solution for your organization to manage all vendors, at all levels of risk exposure.
Benefits of Utilizing the HITRUST Assessment XChange

Cost effective
- Assessment costs carried appropriately by third parties

Efficient
- Offloads burden of administrative and time-consuming activities

Coordinated tracking and management
- Our experts engage your third parties through the process and help answer questions

Contractual obligation compliance
- Unique scoping is available for all third-party requirements

Transparency
- More granular visibility into the security posture of your third parties
- Regular status updates to stay current

Data management and reporting
- Convenient API integration with your existing tools
- Receive and export assessment results
- Get reports on security metrics across your entire third-party population

Our solution harmonizes the various third-party management requirements from all departments across an organization including purchasing, legal, IT, privacy, compliance, and leadership.
Section 6
Provider TPRM
How to Improve Third-Party Risk Management for Your Organization and the Supply Chain Ecosystem

In early 2018, CISOs from leading US-based health provider organizations met to initiate a program to address how organizations like theirs manage and monitor the cybersecurity risks presented by their business associates.

The objectives were clear – we can improve the cyber-security posture of our organizations by:

a. **Bringing uniformity and consistency** to the vendor risk management life cycle (VRMLC) by **simplifying** how CEs and BAs approach and report their cybersecurity risks and controls to one another.

b. **Reducing the cost and increasing the value** our organizations expect from their VRMLC processes by removing wasted time and resources spent on lousy, poorly designed, and inconsistent processes

c. **Aligning our resources** with standards setters, assessors, and monitoring groups to **address hard problems efficiently and be more responsive to emerging threats**

d. **Demonstrating our commitment to industry wide acceptance and adoption** by adopting new practices in our business and promoting them to the industry
Provider TPRM Council

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
Does This Mean I Have to Redo My Security Program?

The HITRUST CSF covers 100% of:

- 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)

HITRUST simplifies the process of aligning from a standard like ISO or NIST to the HITRUST CSF, by providing the *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
- Tens of thousands of HITRUST CSF assessments have been conducted since 2009
- HITRUST CSF assessments are used successfully by organizations to address OCR audits and in support resolution agreements
- HHS specifically references HITRUST’s approach in 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.
HITRUST and SOC 2 Alignment

• HITRUST CSF deemed as suitable criteria
• Assess once, report many
• Combination of standards
• Advantages of a HITRUST assessment compared to a SOC 2
  – Transparency
  – Consistency
  – Accuracy
  – Reliability
  – Forward-looking
Why not 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

Healthcare Sector Implementation of the NIST Cybersecurity Framework (CsF)
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
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 Rapid or Readiness Assessment 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.

Rapid and Readiness Assessments leverage 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.
How Do I Benefit From All This?

- Redundant, inconsistent assessments result in lost productivity and 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
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 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/csf/rmf_risk/MyCSF_vs_GRCTool.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

For more resources, visit the HITRUST Blog at https://blog.hitrustalliance.net
BACKGROUND
Founded in 2007.

HITRUST Alliance, Inc. is a non-profit responsible for frameworks, standards, and methodologies.

HITRUST Services Corporation is a for-profit responsible for training and tools.

ADOPTION
HITRUST CSF is utilized by 81% of US hospitals and health systems and 83% of US health plans.

HITRUST CSF is the most widely adopted control framework in the healthcare industry, according to a 2018 HIMSS survey.

HITRUST CSF Assurance program is the most widely adopted program for assessing third party risk.

BEST KNOWN FOR
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 and Department of Health and Human Services.

- 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.

Operating the healthcare industry 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