HITRUST® Third-Party Risk Management (TPRM) Methodology and HITRUST Assessment XChange™ Enhancements

Wednesday, December 11, 2019

1:00 pm-2:00pm CT

Presenters

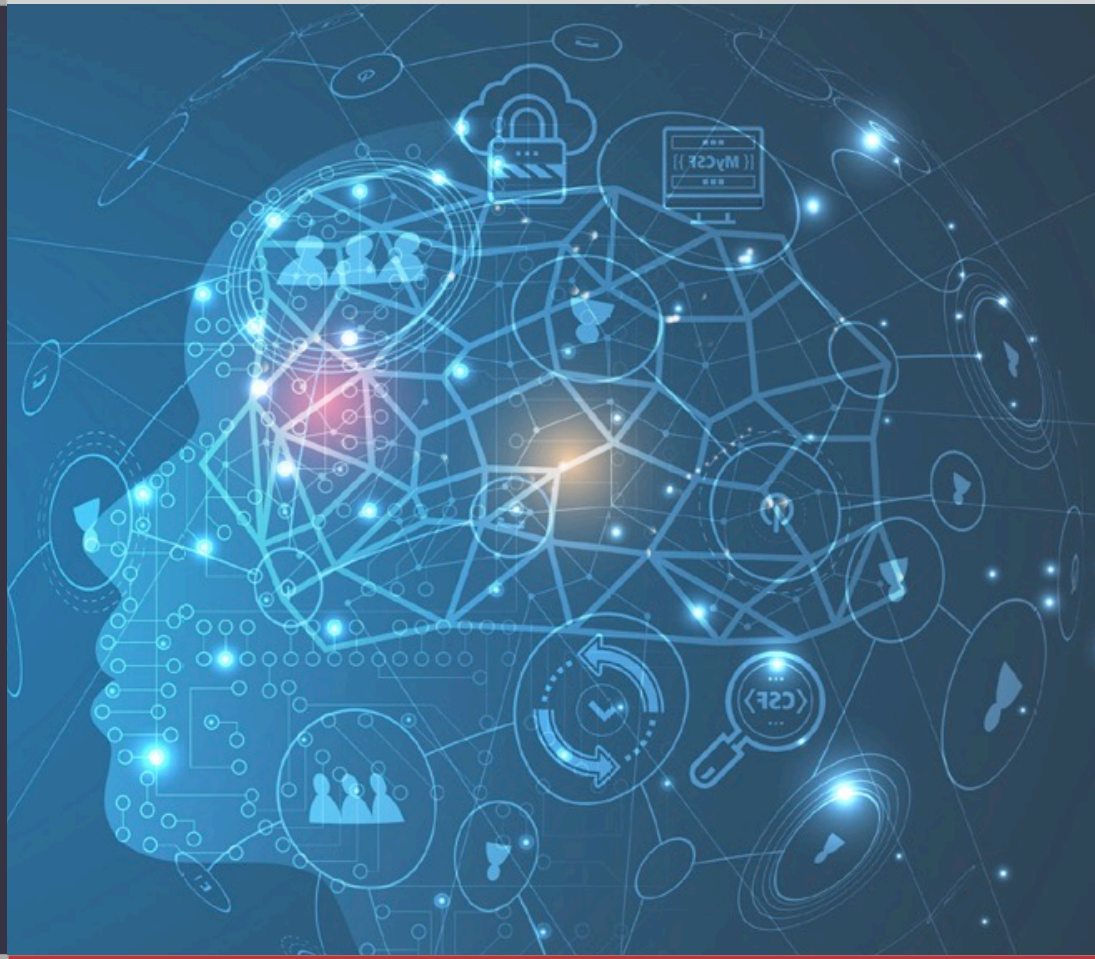
Bryan Cline, Ph.D.
Chief Research Officer, HITRUST

Michael Parisi
VP of Assurance Strategy & Community Development, HITRUST

Jacob Bustos
Director of Vendor Risk Management, HITRUST

Learning Objectives

- How the HITRUST TPRM Methodology and HITRUST Approach helps organizations qualify their third parties for a new business relationship and requalify those with an existing one based on the inherent risk they pose to the organization
- How to utilize the new Inherent Risk Questionnaire and HITRUST CSF Rapid Assessment ("Rapid Assessment"), incorporating them into an organization's TPRM alongside the HITRUST CSF Readiness and Validated Assessments
- How the HITRUST Assessment XChange implements the HITRUST TPRM Methodology's vendor qualification process



The HITRUST Third-Party Risk Management Methodology: Qualification Process

What is the HITRUST TPRM Methodology?

A formal approach to effective and efficient management of the risk incurred from third-party relationships in which sensitive information is shared. This consists of a six-step process:

01 **Initiate:** Formal start of an assessment

02 **Collect:** Gathering of information needed to determine inherent risk of a specific business relationship

03 **Qualify:** Formal evaluation of residual risk due to a specific business relationship

04 **Accept:** Formal acceptance of risk

05 **Select:** Selection of a third party (e.g., a vendor) for a specific business relationship or decision to continue with a third party

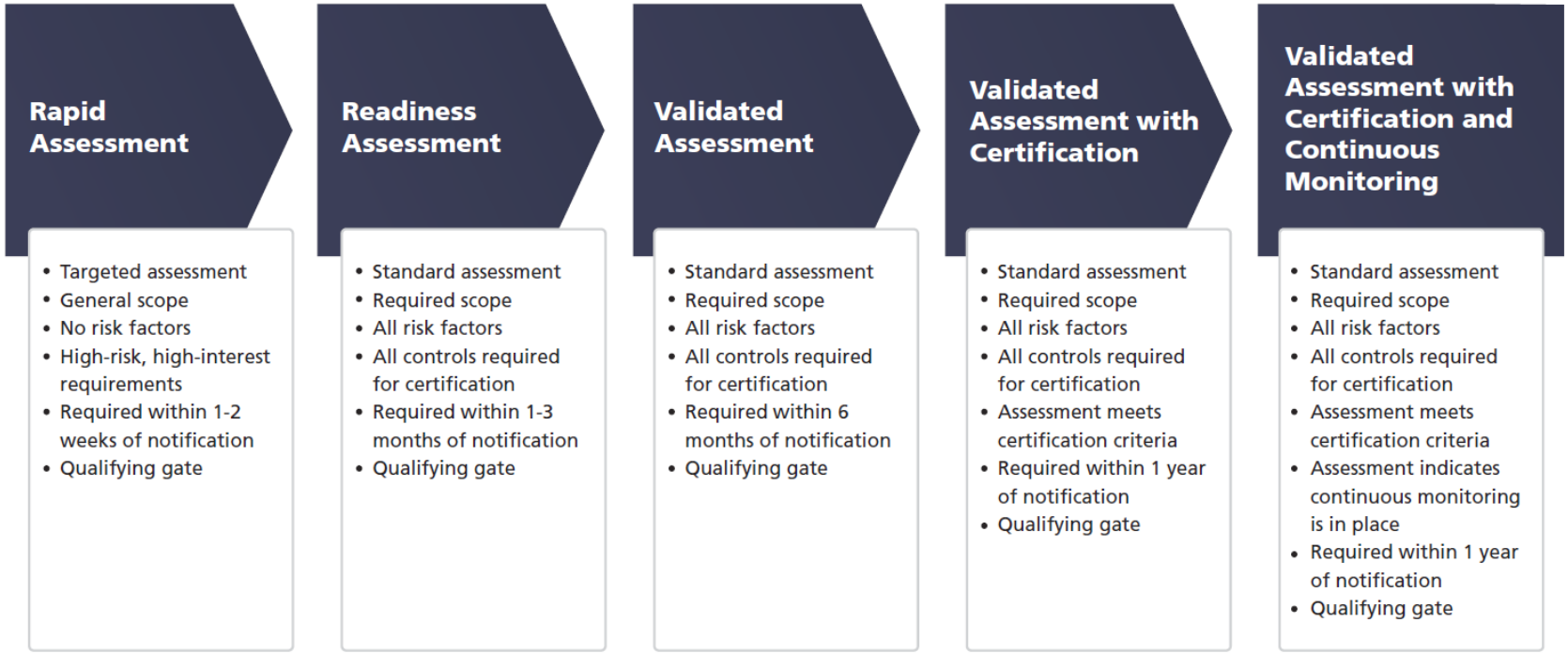
06 **Monitor:** Ongoing monitoring of residual risk

So what exactly does it mean to ‘qualify’ a third party?

The intent of **'Step 3 – Qualify'** is to help an organization:

- Manage its third-party/supplier risk by *qualifying* a third party/supplier
- Based on the inherent risk they represent for a specific business relationship
- Via a specific type of assessment that
- Provides an appropriate (aka satisfactory) level of assurance
- Regarding the amount of residual risk incurred as a result of the business relationship

What types of assessments are used to qualify a third party?



What happens if a third party doesn't have the required assessment?

Although not apparent from the process diagram on a previous slide, qualification is actually an iterative process.

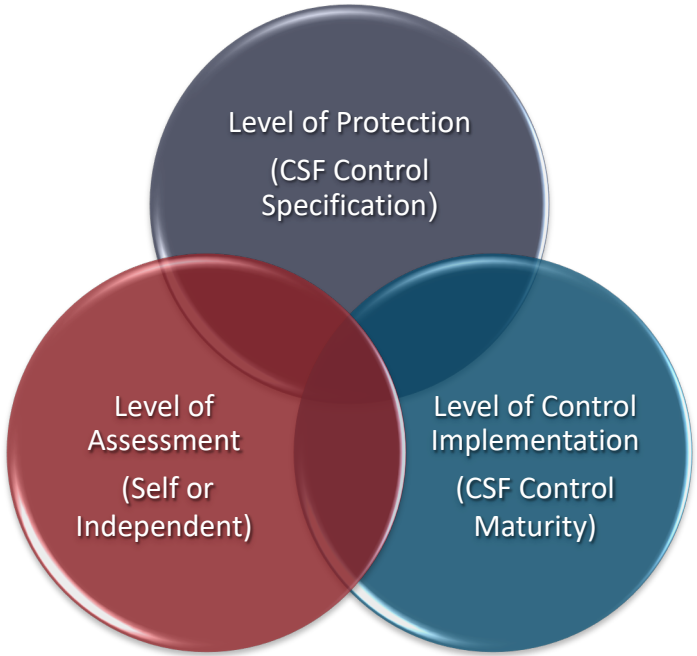
Intent is to provide multiple assurance 'gates' that will allow a third party enough time to obtain an appropriate assessment (subject to an organization's risk appetite, of course).

What new tools are provided for the qualification process?

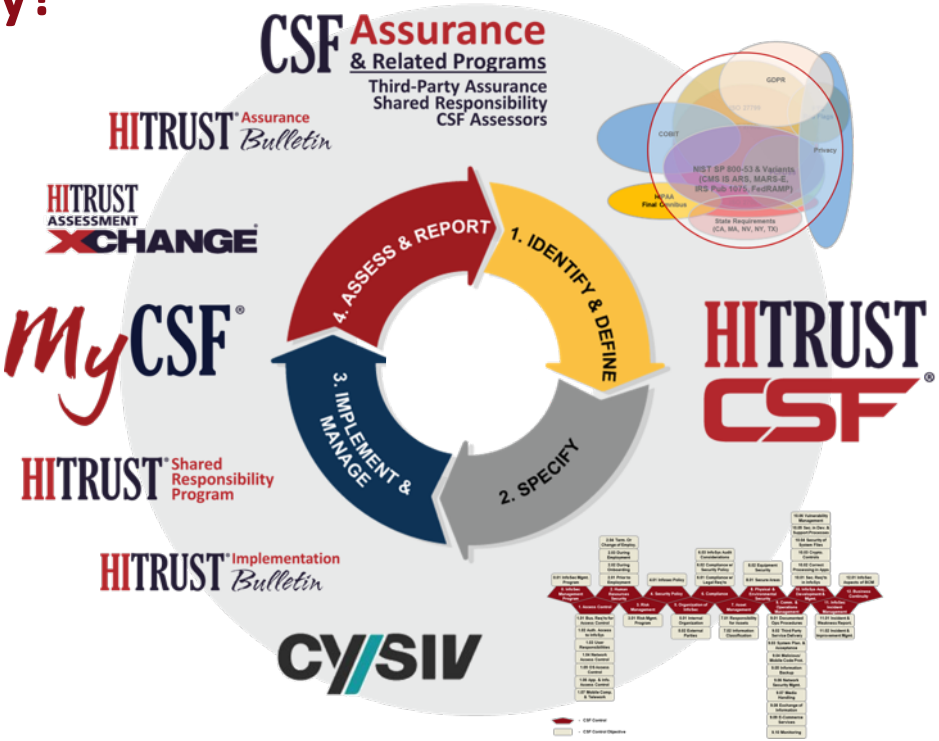
- **Inherent Risk Questionnaire**
  - Used to support risk triage by collecting information on a common set of inherent risk factors—independent of the security and privacy controls that may or may not be implemented by a third party
  - The assurance recommendations also help organizations ensure the remaining residual risk (after controls are applied) does not exceed the organization's risk tolerance
- **Rapid Assessment**
  - A self-attested assessment used to quickly vet the security posture of any third party and that can be answered in a minimal amount of time by the third party
  - Based on 'good security hygiene' practices from the HITRUST CSF® that are suitable for any organization regardless of size or industry
- **HITRUST Trust Score**
  - A new measure that encourages accurate self-assessments by comparing the results of a HITRUST CSF Readiness Assessment with the results of a HITRUST CSF Validated Assessment generated later in the qualification process
  - Provides another useful data point in an organization's evaluation of a third party's information protection program, its overall trustworthiness, and confidence in the assurances provided

Why is the HITRUST TPRM 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)



What else do we need to know about the HITRUST TPRM Methodology?



HITRUST Assessment XChange: Enhancements

What is the HITRUST Assessment XChange?

HITRUST ASSESSMENT XCHANGE™

The HITRUST Assessment XChange ("the 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?

Unlike other offerings, the HITRUST Assessment XChange provides all **3 key components** of TPRM:

01

Industry Agnostic Methodology

The foundation of the XChange is the *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.

02

Expert Support Team

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

03

Innovative Exchange Platform

Powering everything is the user-friendly XChange Manager portal – a secure SaaS platform designed to automate the TPRM qualification process and communications, while streamlining 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.

What are the upcoming enhancements?

The HITRUST Assessment XChange is implementing significant updates in response to customer feedback and market dynamics in an effort to continuously improve our processes and solutions.

Enhancements and New Features:

- ✓ Third-Party Risk Management Methodology (TPRM)
- ✓ Vendor Inherent Risk Questionnaire
- ✓ Rapid Assessment
- ✓ HITRUST Trust Score
- ✓ Assessment Report Request (ARR) Approval Preference
- ✓ Self-Registration in the XChange Manager Portal
- ✓ Ad-Hoc Data Visualization
- ✓ Enhanced Custom Reporting Options

What are the key characteristics of the Inherent Risk Questionnaire?

Inherent Risk Questionnaire – New questionnaire to support risk triage by assessing the inherent risk of a business relationship and determining the appropriate assurance mechanism based on risk being presented by vendor relationship.

The Inherent Risk Questionnaire can be implemented and customized through the XChange Manager platform.

- ✓ A tool that will enable an organization to **properly** assess the inherent risk of its vendor network
- ✓ HITRUST CSF Assessment types recommended based on responses
- ✓ Customer branded questionnaires
- ✓ Ability for a customer to add its own proprietary questions about its business relationships
- ✓ Configurable weighting

What are the key characteristics of a Rapid Assessment?

HITRUST CSF Rapid Assessment – New "pre-qualifying" assessment to quickly vet the security posture of a third party. The Rapid Assessment is industry and framework agnostic, and the data can be leveraged to populate future HITRUST CSF Assessments, reducing inefficiencies.

The Rapid Assessment will be implemented through the HITRUST MyCSF® and the XChange Manager platforms.

- ✓ Can be used when evaluating both new and existing vendors
- ✓ Self-attested assessment – no third-party/assessor validation involved
- ✓ Provides a quick view into a vendor's security posture, in an amount of time determined by the customer
- ✓ Subset of controls that are required for HITRUST CSF Certification
- ✓ Responses will be retained so vendors can re-purpose data to complete future HITRUST CSF Assessments

What are the key characteristics of the HITRUST Trust Score?

HITRUST Trust Score – A score that will be calculated based on results of a vendor's completed HITRUST CSF Readiness Assessment and HIRUST CSF Validated Assessment.

The HITRUST Trust Score will be shared in the XChange Manager platform.

- ✓ Assessments must be of identical scope
- ✓ Score will be shared with both organization and vendor
- ✓ Will encourage vendors to be more accurate in their self-evaluation and ensure their understanding of the requirements
- ✓ Can be used by an organization to evaluate the strength and trustworthiness of its vendor relationships

What is the recommended workflow?

01 Participating Organization (PO) screens vendors to determine which will participate in the qualification process.

02 PO determines which vendors will receive an Inherent Risk Questionnaire (IRQ) and Rapid Assessment.

03 IRQ questions can be parsed out internally to business unit/supply chain or externally to vendor for completion. The Rapid Assessment is sent to the vendor for completion by the deadline set by the PO.

04 The IRQ allows for a customized, auto-generated assurance recommendation for each vendor.

05 The IRQ serves as the foundation for each vendor's next steps, based on the risk to the PO. Scores are generated automatically in the HITRUST Assessment XChange Manager platform.

06 The table below specifies recommended levels of assurances based on the Inherent Risk Score. The PO has the ability to override the recommended assessment on a one-off basis. Overrides require Management approval from the PO.

Inherent Risk	Assurance Approach
0 – Very Low	HITRUST CSF Readiness Assessment w/ No Minimum Score and CAPs Not Required
1 – Low	HITRUST CSF Validated Assessment with No Minimum Score and CAPs Allowed
2 – Moderate	HITRUST CSF Validated Assessment > 62 w/ CAPs Allowed
3 – High	HITRUST CSF Validated Assessment ≥ 71 w/ No CAPs Allowed
4 – Very High	HITRUST CSF Validated Assessment ≥ 87 w/ CAPs Allowed

UPCOMING MARKET-FACING EVENTS

HITRUST 2020

COLLABORATE

Learn. Collaborate. Deliver.

Date: May 19-21, 2020

Location: Gaylord Texan Resort & Convention Center

Registration opens January 6, 2020 – *Mark your calendar!*

Attendee Q&A

Additional Resources

HITRUST TPRM Methodology: Qualification Process Whitepaper
Provides the latest iteration of the HITRUST TPRM Methodology
https://hitrustalliance.net/content/uploads/TPRM-Methodology.pdf

Leveraging a Control-Based Framework to Simplify the Risk Analysis Process
Discusses the HIPAA risk analysis, its purpose, and how a controls-based risk management framework can be leveraged to satisfy due-diligence and due-care obligations and comply with HIPAA
https://hitrustalliance.net/content/uploads/2016/01/Leveraging-a-Control-Based-Framework-to-Simplify-the-Risk-Analysis-Process.pdf

Risk Analysis Guide for HITRUST Assessors and Organizations
Provides a complete treatment of HITRUST's approach to risk analysis and control gap assessments
https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf

HITRUST®

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight