HITRUST®

Third-Party Risk Management

Methodologies, Programs and Services

Topics

- The Problem with TPRM Today
- HITRUST’s Solution for TPRM
- Key HITRUST Differentiators
- Getting Started with HITRUST TPRM

The Problem with TPRM Today

The Need for Third-Party Risk Management (TPRM)

The need for organizations to proactively evaluate and manage the business risks they incur by sharing sensitive and regulated information with vendors, suppliers and other third parties continues to grow due to:

- – Evolving cyber threats
- – Expanding regulations
- – Increasing levels of data access
- – Expanding supply chains
- – Rising number & cost of data breaches

How are we possibly going to manage all this? We probably have hundreds of third parties!
We really need to figure out how much risk we incur by sharing information with each of our third parties, because they are all different.
Sure . . . but where do we start? How do we start?
That makes sense. We share a lot of information with a few of our vendors and very little with most of them.

The Current State of TPRM

- Organizations managing third-party risk face these challenges:
  - Unknown risk profile
  - Multiple & disparate questionnaires and assessment approaches
  - Inappropriate or inconsistent level of assurance
  - Inaccurate estimates of risk
  - Time-consuming
  - Costly to manage
- TPRM solutions today are simply inconsistent, generally inefficient (if not ineffective), and often unaffordable at scale

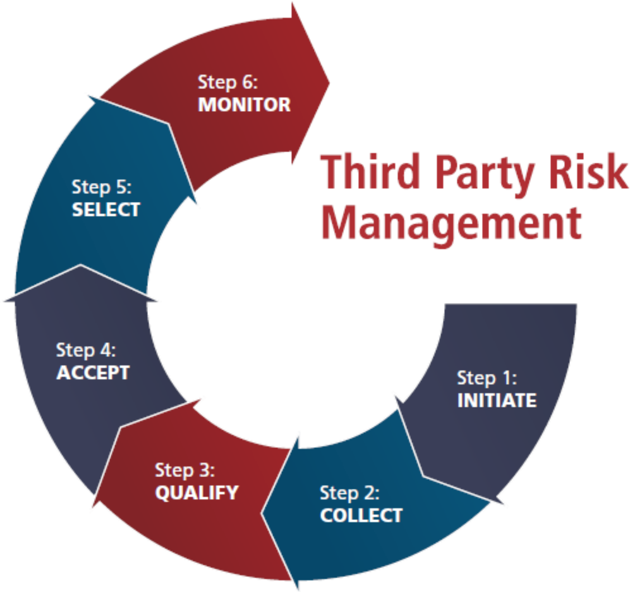
Improving the State of TPRM

- TPRM should be:
  - Standardized and transparent for consistency
  - Broadly applicable and scalable to any size and type of third-party
  - Flexible in providing various levels of assurance
  - Accurate in how they reflect a third-party's security posture
  - 'Rely-able' across different types of stakeholders
  - Cost-effective for organizations and third-parties alike

HITRUST’s Solution to the TPRM Problem

What organizations and third parties need is the consistency, efficiency, effectiveness and affordability provided by the HITRUST TPRM Program

HITRUST TPRM Methodology



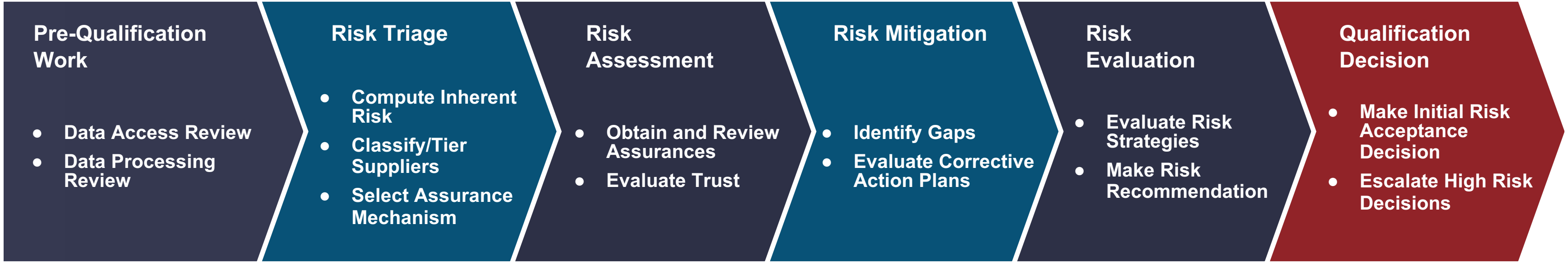
- A formal approach to effective and efficient management of third-party risk
- Consists of a six-step process
  1. **Initiate**: Formal start of the TPRM process
  2. **Collect:** Gathering of information needed to determine risk of a specific business relationship
  3. **Qualify**: Formal evaluation of risk due to a specific business relationship
  4. **Accept**: Formal acceptance of risk
  5. **Select**: Selection of a third party (e.g., a vendor) for a specific business relationship or decision to continue with a third party
  6. **Monitor**: Ongoing monitoring of risk
- Satisfies HITRUST CSF requirements for TPRM

‘Qualifying’ a Third Party

Expanding on Step 3 of the TPRM Methodology

The intent of ‘qualification’ is to help an organization manage its third parties …

- Based on the inherent risk they represent for a specific business relationship …
- Via a specific type of assessment that …
- Provides an appropriate (i.e., satisfactory) level of assurance …
- Regarding the amount of residual risk incurred as a result of the business relationship …
- By mitigating inherent risk through implementation of reasonable and appropriate safeguards



Pre-Qualification Work

- Data Access Review
- Data Processing Review

Risk Triage

- Compute Inherent Risk
- Classify/Tier Suppliers
- Select Assurance Mechanism

Risk Assessment

- Obtain and Review Assurances
- Evaluate Trust

Risk Mitigation

- Identify Gaps
- Evaluate Corrective Action Plans

Risk Evaluation

- Evaluate Risk Strategies
- Make Risk Recommendation

Qualification Decision

- Make Initial Risk Acceptance Decision
- Escalate High Risk Decisions

TPRM Step 3 - Qualify

HITRUST Programs Supporting TPRM ‘Qualification’

TPRM Qualification Process Step	HITRUST ASSESSMENT XCHANGE	CSF ASSURANCE PROGRAM™	MyCSF	HITRUST CSF
Pre-Qualification Work	• XChange Support Team • Workflow Management			
Risk Triage	• IRQ • Inherent Risk Score • Assurance Recommendation • Workflow Management			
Risk Assessment	• Rapid Assessment • Trust Score • Workflow Management	• Assessment Methodology • Internal & External Assessors	• Readiness Assessment • Validated Assessment • Validated w/ Certification • API Support	• Risk-based Control Selection
Risk Mitigation	• Dashboards & Reports • Corrective Action Plans (CAPS)		• Risk Treatments • CAPs • API Support	
Risk Evaluation	• Dashboards & Reports • Workflow Management			
Qualification Decision	• Dashboards & Reports • Workflow Management			

Definitions of tools available here.

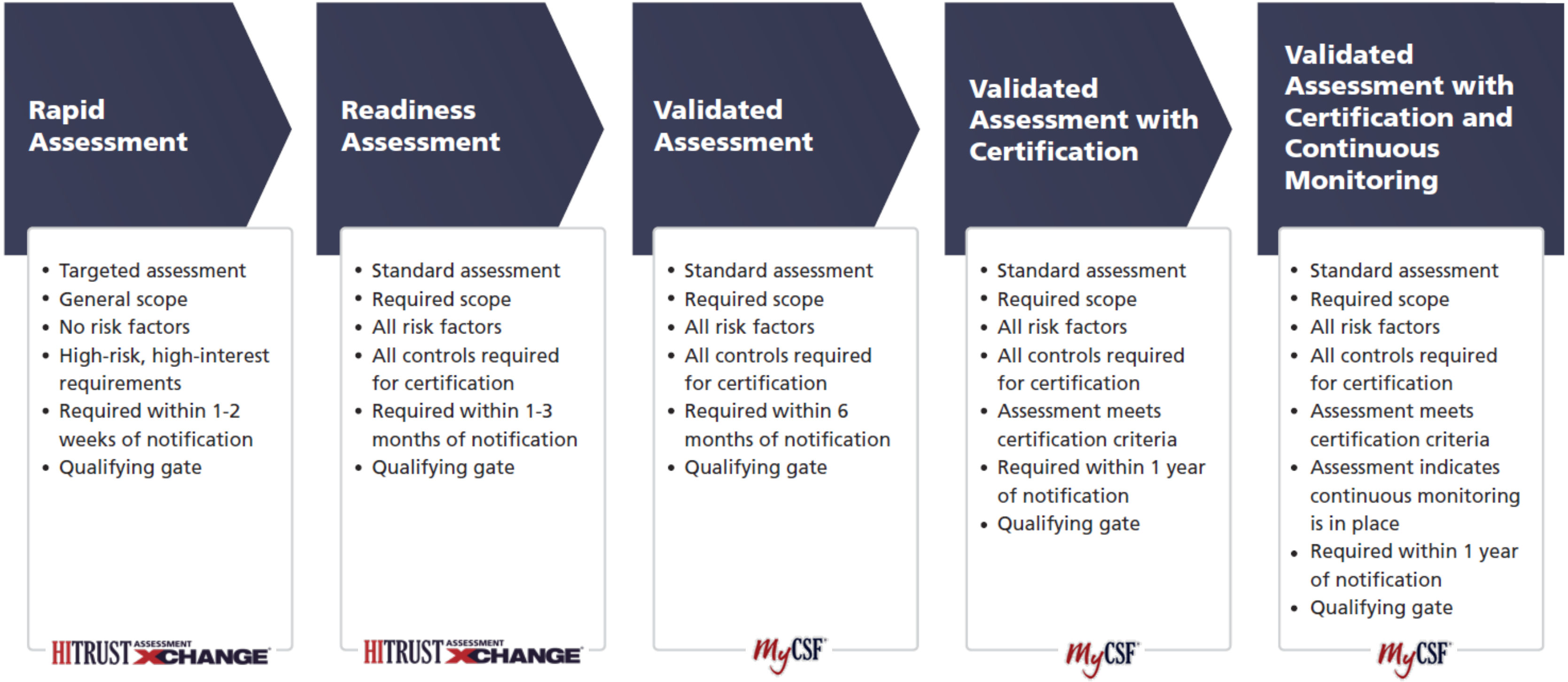
Getting Ready for ‘Qualification’

- Gather and review information about the third party and the business relationship
  - Examples include proposals, contracts and other documentation that describe the information that will be processed and how it will be processed
  - Additional information about the third party such as size, jurisdiction, and financial health may be needed to facilitate the entire qualification process
- The HITRUST Assessment XChange (‘the XChange’) support team can help
  - Identify appropriate third-party contacts
  - Communicate requirements
  - Educate your third parties on the process and your expectations
  - Ensure your organization is only engaged when a third party is not meeting its obligations

Triaging Inherent Risk

- Inherent risk is based on ‘factors’ related to engaging in a specific activity
  - Examples include amount of data shared, type of processing, and potential fines/penalties
- The XChange can provide automated support for the entire ‘risk triage’ process
  - An *Inherent Risk Questionnaire (IRQ)* helps collect relevant information
  - An *inherent risk score* is calculated based on the information collected
  - Specific *assurance recommendations* are made based on the resulting score
    - The type and rigor of assessment is specified ‘up front’, e.g., a HITRUST CSF Validated Assessment
    - Specific HITRUST CSF information protection requirements are based on the assessment scope (determined when the assessment is generated in MyCSF)
- The HITRUST TPRM approach can quickly triage potential risk and recommend appropriate assurance requirements for all your third parties

Available ‘Qualification’ Assessments



Rapid Assessment

- Targeted assessment
- General scope
- No risk factors
- High-risk, high-interest requirements
- Required within 1-2 weeks of notification
- Qualifying gate

HITRUST ASSESSMENT XCHANGE

Readiness Assessment

- Standard assessment
- Required scope
- All risk factors
- All controls required for certification
- Required within 1-3 months of notification
- Qualifying gate

HITRUST ASSESSMENT XCHANGE

Validated Assessment

- Standard assessment
- Required scope
- All risk factors
- All controls required for certification
- Required within 6 months of notification
- Qualifying gate

MyCSF

Validated Assessment with Certification

- Standard assessment
- Required scope
- All risk factors
- All controls required for certification
- Assessment meets certification criteria
- Required within 1 year of notification
- Qualifying gate

MyCSF

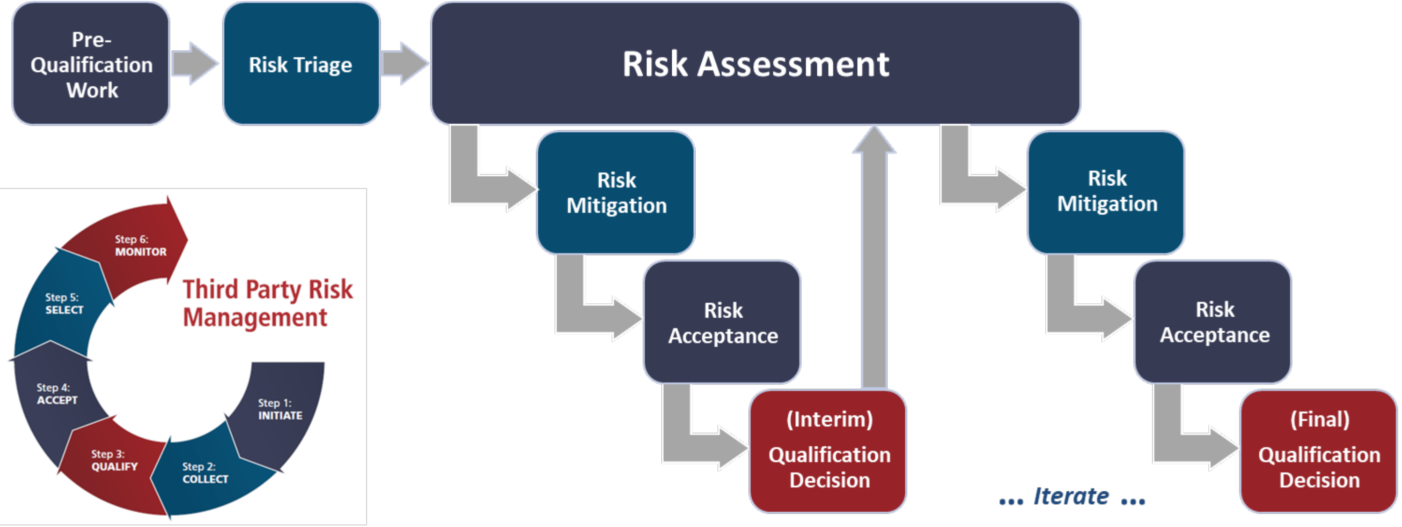
Validated Assessment with Certification and Continuous Monitoring

- Standard assessment
- Required scope
- All risk factors
- All controls required for certification
- Assessment meets certification criteria
- Assessment indicates continuous monitoring is in place
- Required within 1 year of notification
- Qualifying gate

MyCSF

Iterative Assurance Process

- Third-party ‘qualification’ is an iterative process with multiple approval ‘gates’



Pre-Qualification Work

Risk Triage

Risk Assessment

Risk Mitigation

Risk Acceptance

(Interim) Qualification Decision

... Iterate ...

Risk Mitigation

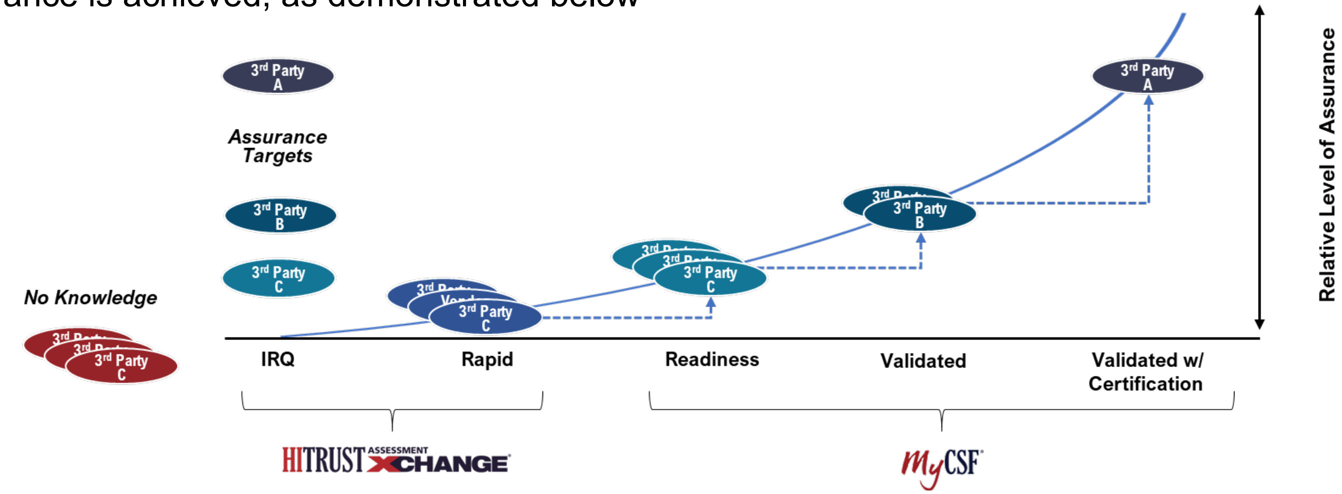
Risk Acceptance

(Final) Qualification Decision

- Iteration allows a third-party the time needed to provide appropriate assurances while addressing concerns about excessive risk throughout the qualification process

Iterative Assurance Process (Continued)

- The XChange can help automate requests, workflow management, and reporting until the required level of assurance is achieved, as demonstrated below



Iterative Assessment Process

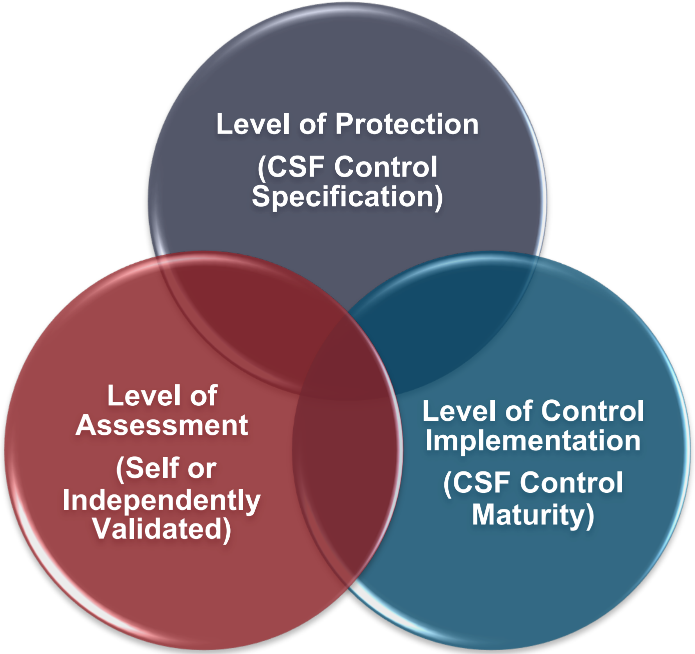
- The XChange also provides a Rapid Assessment and Trust Score to support iterative assurances
  - A Rapid Assessment to quickly determine if basic ‘good security hygiene’ practices are in place
  - A Trust Score to help ensure the ‘rely-ability’ of self-attested HITRUST CSF Readiness Assessments

Mitigating and Managing Risk

- Identify deficiencies or ‘gaps’ in implementation of required controls with each assessment and develop, evaluate and update corrective action plans (CAPs) as needed
  - Required CAPs are provided in every HITRUST CSF Readiness and Validated Report produced in MyCSF, delivered electronically in the HITRUST Assessment XChange and easily ported to other GRC solutions
- Periodically review control implementation status to determine if risk is being treated appropriately
  - The HITRUST Assessment XChange provides additional workflow management, dashboards and reports to help track risk treatments and progress towards completing required CAPs and mitigating excessive levels of risk
- Each time the risk management strategy is evaluated after an assessment and until the iterative assurance process is complete, use the results to qualify the third party for continued assessment or, based on the final assessment, formally qualify the third party for the business relationship
  - The HITRUST Assessment XChange provides constant visibility into your third party's assessment status throughout the qualification process through various dashboards and reports to provide the information needed to make an interim or final third-party qualification decision
    - Excessive residual risk is estimated based on the HITRUST CSF control requirements that are not fully implemented
    - Third-parties are generally qualified when the residual risk does not exceed their specific risk appetite or tolerances

Key HITRUST TPRM Program Differentiators

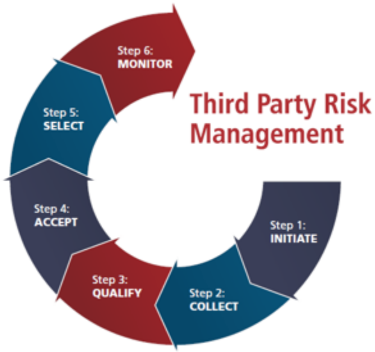
- Simple, open model based on inherent risk of the relationship
- Leverages the HITRUST CSF
  - Demonstrates appropriate level of due diligence
- Leverages the HITRUST CSF Assurance Program
  - Demonstrates appropriate due care
- Reduces costs for TPRM programs
  - Reduces need for / scope of internal resources
- Reduces costs for third parties
  - “Assess Once, Report Many™”
- Supports three dimensions of assurance


Level of Protection
(CSF Control Specification)
Level of Assessment
(Self or Independently Validated)
Level of Control Implementation
(CSF Control Maturity)

Getting Started with HITRUST TPRM

The Only Comprehensive, Modular & Integrated Solution

HITRUST provides all the components needed to help organizations manage third-party risk efficiently and effectively, whether it's simply to keep track of their third-parties, identify an appropriate set of information protection requirements, or help obtain a level of assurance appropriate to the risk they pose.



Third Party Risk Management

Step 1: INITIATE

Step 2: COLLECT

Step 3: QUALIFY

Step 4: ACCEPT

Step 5: SELECT

Step 6: MONITOR

CSF ASSURANCE PROGRAM™

HITRUST CSF®

MyCSF®

HITRUST ASSESSMENT XCHANGE®

Adopt What You Need, When You Need It

- For example, you can simply:
  - Accept HITRUST CSF reports in lieu of your proprietary questionnaire
  - Require HITRUST CSF reports from your third-parties
  - Use the IRQ to understand the inherent risk posed by your third-party relationships
  - Use the Rapid Assessment to quickly gauge the security posture of third-parties
  - Leverage the XChange to help keep track of your third-parties
  - Integrate elements of the HITRUST TPRM Methodology into your TPRM program
  - Use the XChange to facilitate formal management of your third-parties
- How you use the various tools, products and services provided by the HITRUST TPRM Program is customizable based on your specific requirements and preferences
- How can we help?

Learn More

- More information on the HITRUST approach to TPRM is available from these resources:
  - Solving the TPRM Problem
  - The HITRUST TPRM Program
  - TPRM Methodology Qualification Process
- The latest version of the HITRUST CSF
- Learn more about the HITRUST CSF Assurance Program
- Information on MyCSF and its capabilities
- Find out more about the HITRUST Assurance XChange

Call us directly
1-855-HITRUST

Email us
info@HITRUSTAlliance.net

View more resources
HITRUSTAlliance.net

HITRUST®

HITRUSTAlliance.net