HITRUST®

HANDBOOK for Managing Vendor Information Risk

Overview reference for optimizing the HITRUST qualification process to efficiently use our assessment portfolio

HITRUST TPRM Implementation: Handbook v.1

How organizations and TPRM software solution providers can ensure due diligence and due care when leveraging the six-step HITRUST TPRM Methodology

October 2022

Patent Pending Methodology

Proprietary HITRUST process uses a well-defined quasi-quantitative risk analysis approach combining our unique methodology with Assurance Rely-Ability™ Maturity Model (ARMM) scoring to identify and evaluate vendor risk.

Table of Contents

For Additional Information

HITRUST TPRM Implementation Quick-Start Guide

Streamlined, at a-glance resource provides a foundational introduction to our approach, along with a high-level overview of initial adoption stages.

For Additional Information

HITRUST Methodology Guide for Managing Vendor Information Risk

In-depth process document that classifies, assesses, computes, mitigates, and evaluates third-party inherent risk.

Table of Contents

List of Figures

List of Tables

Introduction

HITRUST is a globally recognized leader in information risk management and assurance reporting. Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security, and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks as well as related assessment and assurance methodologies.

The HITRUST Third-Party Risk Management (TPRM) Methodology—or simply 'the methodology'—is presented in a separate HITRUST whitepaper[1]—which we'll refer to as the 'whitepaper' going forward—and provides industry with a common, consistent approach to determining what information risk assurances should be provided and maintained when an organization shares sensitive information with a third party. It specifically addresses systemic inefficiencies that occur when organizations seek greater assurances from their third parties than is warranted based on risk or regulatory compliance requirements or insufficient assurances and expose themselves to more risk than intended based on their tolerance or capacity to accept risk.

The HITRUST TPRM Implementation Handbook—hereinafter referred to as 'the handbook'—is a companion to the HITRUST whitepaper and focuses on how organizations should integrate the methodology into their existing third-party onboarding processes to qualify or requalify third parties for a specific business relationship by obtaining assurances appropriate to the information security, privacy, and compliance risk these third parties inherently pose.

More specifically, in this handbook, we discuss:

- Various considerations for methodology and technology adoption
- The relationship between levels of inherent risk and reliable assurances
- The level of assurance needed from a third party to ensure an appropriate standard of care
- Balancing disparate risk tolerances with the need for an appropriate standard of care
- Iterating through progressively more reliable assessments until the requisite level of assurance is achieved
- The value of a single control framework and assurance program with TPRM
- The benefits of third parties traversing the HITRUST Portfolio
- Where each HITRUST assessment fits in the methodology

The handbook also highlights key points that application developers should consider when developing new products, services, and tools around the methodology or integrating the HITRUST TPRM methodology into existing ones to ensure their customers have an appropriate amount of flexibility in managing third-party risk while maintaining an appropriate level of due diligence and due care.

And, since the handbook relies heavily upon the discussion of the methodology in the whitepaper, it should be viewed as a companion or supplement to the whitepaper rather than a standalone reference. We subsequently do not repeat content in the previous work unnecessarily and instead focus our discussion on the issues we believe are most relevant to the methodology's implementation.

[1] Cline, B. (2022, Jul). *The HITRUST Third-Party Risk Management (TPRM) Methodology: The Qualification Process, Version 2.1*: A streamlined approach to qualifying a third party for a business relationship leveraging the HITRUST CSF and HITRUST Assurance Program. Frisco, TX: HITRUST.

Standard of Care

Third parties such as vendors, suppliers, service providers, and business partners, can introduce significant business risk to an organization simply due to the type and amount of sensitive information provided and how they process and potentially share this information amongst themselves. Organizations subsequently have an obligation to ensure the risk posed by these third parties is adequately mitigated as part of a generally acceptable standard of care for the protection of sensitive information.

By 'standard of care,' we mean "the degree of care or competence that one is expected to exercise in a particular circumstance or role"[2] under the circumstances. If one fails to meet an applicable standard of care and causes harm to another, one could be considered negligent and subsequently held liable for such harm.[3] In the context of the standard of care for TPRM, an organization should apply an appropriate level of due care and due diligence when qualifying (i.e., assessing, evaluating, and accepting) and re-qualifying third parties for an existing or future business relationship. This is especially important when a duty of care is established by relevant law, regulation, or contractual agreement.

For our purposes, an organization exercises due care—the conduct that a reasonable man or woman will exercise in a particular situation to protect others[4]—by implementing a methodology through policies and procedures that will help them manage third-party risk appropriately. It exercises due diligence— the care that a reasonable person takes to avoid harm[5]—when applying the methodology to ensure specific third parties present an appropriate level of residual risk based on their specific business relationships on an ongoing basis.

The HITRUST methodology's qualification process triages and scores the level of risk inherent in sharing information with a third party (e.g., its sensitivity and criticality) and how it intends to process the information (e.g., remote access by a cloud service). The inherent risk scores are then equated with Rely-Ability™ scores for available assurance approaches, e.g., the HITRUST Assessment portfolio, based on specific features of the approach that contribute to its overall rigor (e.g., accuracy and precision of assessment results), impartiality (e.g., independence of the assessor), and suitability (e.g., relevancy of assessed controls to the relying party).

By objectively and transparently identifying assurance methods that are appropriate to the level of risk presented by a third party, the HITRUST TPRM Methodology is uniquely positioned to help organizations provide an appropriate industry-acceptable standard of care for the information they entrust to a third party. However, its ability to do so is highly dependent on how well the methodology is adopted and subsequently integrated into organizational TPRM processes and supporting applications.

[2] Merriam-Webster (2022a). Standard of Care. In *Merriam-Webster.com legal dictionary.*
[3] Cornell Law School (2021, Sep). *Standard of Care. In Legal Information Institute law dictionary.*
[4] Merriam-Webster (2022b). Due Care. In *Merriam-Webster.com legal dictionary.*
[5] Merriam-Webster (2022c). Due Care. In *Merriam-Webster.com legal dictionary.*

Implementing a Methodology

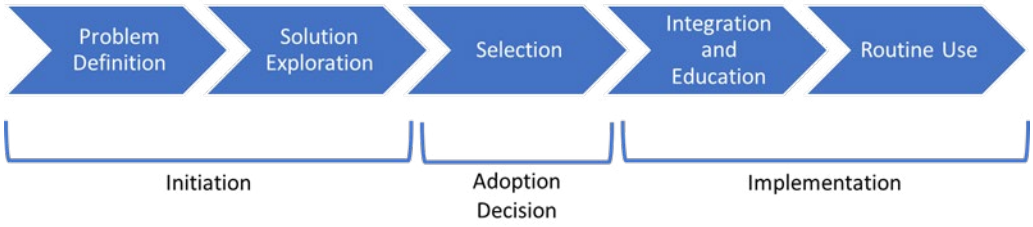
The intent of this implementation handbook is to ensure organizations adopting the HITRUST TPRM Qualification Methodology do so in a way that ensures a minimally acceptable standard of care as described in the previous section. However, anyone that has been involved in the adoption of a new methodology—whether something as grand as Total Quality Management (TQM) or something more modest like changing a single existing business process—understands there is more to making the adoption successful than simply making the decision to do so.

This is because organizations are generally resistant to change, even if it believes change is necessary. For example, third parties that were not required to provide assurances around their information protection programs before implementation of the HITRUST TPRM Qualification Methodology may not understand why the change is necessary and subsequently not want to provide those assurances. The same could be said for organizations that may be asked to provide more robust assurances such as a third-party assessment when they were previously only required to self-assess. Organization stakeholders may also not understand why they need to implement a program that addresses their entire third-party population or how the benefits may outweigh the cost and effort of adopting the methodology innovation.

Fortunately, there is an extensive amount of literature on organizational change and innovation adoption that can help us understand how to improve the likelihood that adoption of any methodology, including this one, will be successful.[6]

Innovation adoption can be thought of as a process with five major steps, as shown in Figure 1 below.

Figure 1. Innovation Adoption Process[7]



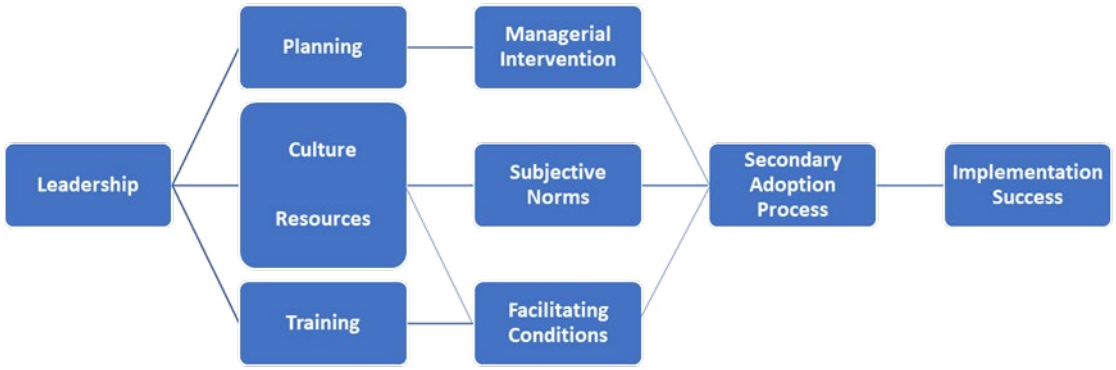
Following the process from left to right, an organization first recognizes it has a problem or need for an innovation, after which it goes about matching prospective innovations to that problem or need. A decision is made by selecting a particular innovation, which results in the organization redefining or restructuring itself to integrate or otherwise accommodate the innovation. The organization's workforce is educated on the innovation, after which members begin to use the innovation until such use is as a matter of routine.

We assume an organization has already made the decision to adopt the HITRUST TPRM Qualification Methodology and subsequently focus this handbook on factors related to the integration of the methodology's activities into existing business processes for procurement and contracting in general and TPRM in particular.

At a basic level, there are essentially five factors related to the adoption of a methodology innovation that help organizations overcome an inherent resistance to change from the 'status quo' and successfully implement the methodology.

[6] Cline, B. (2008). Factors Related to the Implementation of Information Systems Security Engineering: A Quality Perspective. [Doctoral dissertation, University of Fairfax], pp. 50 – 96.
[7] Adapted from Cline, B. (2008), p. 53.

Figure 2. Methodology Adoption Factor and Process Model[8]



As seen in Figure 2 above, a single factor—leadership—influences the other four factors: planning, (organizational) culture, resources, and training (or 'education' per the innovation adoption process depicted earlier in Figure 1). Without leadership support, planning would likely not be adequate to the task, a culture resistant to change would remain resistant, and adequate resources and training would not be provided to support the implementation.

Adequate planning helps ensure management becomes involved when problems with implementation occur. Culture and resources work together (a statistical interaction occurs between these two factors) to help address the organization's subjective norms, which is best described in this context as 'perceived social pressure' for specific types of behaviors. And training (education) helps inform stakeholders (e.g., users) on why the organization is adopting the methodology and how to use it, which helps set the conditions for subsequent acceptance of the methodology by various stakeholders. By positively influencing management involvement in the methodology's implementation and integration with organizational processes, encouraging appropriate behaviors from the workforce regarding use of the methodology, and educating stakeholders and training the workforce in its use, the organization influences secondary adoption of the methodology by each individual stakeholder, which ultimately results in its routine use—the last stage of the innovation adoption process.

By understanding these factors and addressing them during the methodology implementation process, organizations can help ensure the implementation is not only successful, but also what they implement will provide a minimally acceptable standard of care as intended by the organization.

[8] Cline, B. (2008), p. 185.

The Qualification Process

Many organizations address third-party risk through a formal management process such as the one used in the HITRUST TPRM Methodology shown in Figure 3 below.

Figure 3. HITRUST TPRM Process

While the actual implementation of TPRM varies from one organization to another, they will typically address each step of the process in some way.

- Step 1 – **Initiate.** Prior to contract award or as part of a routine or special reassessment (e.g., annually or after a material change in the relationship, respectively), formally initiate the TPRM process and, if necessary, request information from internal departments or external stakeholders.
- Step 2 – **Collect.** Gather proposals, contracts, and other documentation about the third party and the products, services, etc., the third party provides or will provide, including documentation received from the third party (e.g., a short questionnaire about their business practices) and then route to the SMEs within the organization for review.
- Step 3 – **Qualify.** Evaluate the information about the third party and the products, services, etc., the third party provides or will provide and assess the level of risk they pose to the organization.
- Step 4 – **Accept.** Formally accept or decline to accept the level of risk posed to the organization should they enter or continue a formal relationship (for the products, services, etc., provided). Note that failure to accept the risk should result in dropping the third party from consideration in a competitive bid or canceling/modifying the contract or other agreement if a current relationship exists.
- Step 5 – **Select.** If entering into a new relationship via competitive selection, select the appropriate third party, execute all necessary legal contracts, and complete other onboarding activities; if an existing relationship, make any changes needed in legal contracts or other documentation to reflect any changes in the third-party relationship (e.g., the amount of data the third party receives or how it is processed).
- Step 6 – **Monitor.** Continuously monitor the third party for changes in potential business risk, including information security, privacy, and compliance risk.

Organizations will re-enter the Initiate step to review existing third-party relationships and determine if there have been any material changes in the relationship either periodically (e.g., annually) or aperiodically when a specific condition or trigger is encountered (e.g., a third party reports a breach).

The HITRUST TPRM Methodology currently focuses on the third step, Qualify, which is itself a process consisting of six steps as shown in Figure 4, and is used to vet a third party for a business relationship by evaluating information about the third party and the products, services, etc., it provides or will provide as well as assessing the level of risk it poses to the organization given the information it processes or will process.

Figure 4. Third-Party Qualification Process

The qualification process depicted above consists of six basic steps:

1. Pre-Qualification Work (PQW) – Data access is reviewed based on the information gathered in the prior step in the TPRM process model;
2. Risk Triage (RT) – The third party is classified or tiered according to the level of inherent risk it presents based on specific risk factors;
3. Risk Assessment (RA) – Assurances around the level of residual risk the third party poses to the organization based on an attestation or assessment of conformity to an organization-defined security and privacy standard are obtained and reviewed;
4. Risk Mitigation (RM) – Any gaps in conformity are evaluated along with the third party's corrective action plans (CAPs) to address those gaps, if any;
5. Risk Evaluation (RA) – The remaining or residual risk is evaluated, and a recommendation is made to either accept or reject the residual risk; and
6. Qualification Recommendation (QR) – A recommendation is made to either accept or decline to accept that risk based on its general risk appetite and specific risk tolerances.

Although we will address each of these six steps in some way, the handbook primarily focuses on how organizations should triage risk, specify an appropriate level of assurance, and then obtain those assurances in order to support a qualification decision, i.e., whether or not the risk associated with a particular third-party business relationship is acceptable to the organization or not.

Qualify Step 1 – Pre-Qualification Work

Figure 5. Qualify Step 1 - Pre-Qualification Work

Pre-qualification work is triggered when a third party is submitted for qualification in support of a proposed or existing business relationship. The intent of this step is to pull existing information from available systems, databases, and other information repositories (e.g., contracting, procurement, TPRM, and information technology (IT)) that is needed to support the next step in the process, risk triage. When information is not available, the organization's TPRM analyst will need to query business owners, IT personnel, contracting/procurement personnel, and the target third party (or parties) for the subject business relationship under consideration. Once the appropriate information is available, the information is then submitted to the TPRM system for risk triage.

DEVELOPER TIP: Qualification may be initiated manually or automatically if the organization's TPRM system is interfaced with its contracting, procurement, or third-party (vendor) management system(s), as applicable. If initiation is automatic, HITRUST recommends alerting the responsible TPRM analyst and other organization-selected personnel and retaining the ability to manually initiate, hold, or override initiation when needed. The system should also have the capability to receive structured and unstructured information from the organization's contracting, procurement, and/or third-party (vendor) management systems.

Qualify Step 2 – Risk Triage

Figure 6. Qualify Step 2 – Risk Triage

Triage may begin automatically once all requisite information is available in the organization's TPRM system or it may be initiated manually as with the pre-qualification work.

HITRUST's triage approach—current as of the handbook's date of publication—is shown in Table 1 on the following page. Three types of risk factors are used: organizational and compliance risk factors help us estimate the impact component of inherent risk and technical risk factors help estimate potential impact.

The inherent risk posed by a third party is evaluated based on simple averages of these factors and a normalized score is produced between zero and five, which is then used to categorize the inherent risk of a business relationship into six tiers.

$$Inherent\ Risk\ Score = ROUND\left[\frac{Likelihood\ x\ Impact}{5}\right]$$

DEVELOPER TIP: HITRUST recommends the organization's TPRM system automatically alert the responsible TPRM analyst and other organization-selected personnel when the inherent risk triage scores and associated assurance recommendations have been generated.

Table 1. HITRUST TPRM Triage Model

Risk Component	Risk Factor Type	Risk Factor	Risk Factor Ratings						Risk Factor Score	Risk Component Score	Risk Score
			None - 0	Very Low - 1	Low - 2	Medium - 3	High - 4	Very High - 5			
Impact	Organizational	IO1: Percentage of organizational data	None or N/A	0% < 20%	20% < 40%	40% < 60%	60% < 80%	> 80% or Unknown	Simple Average	Simple Average	Simple Average
		IO2: Total amount of organizational data	None or N/A	< 1M records	1M < 10M Records	10M < 30M Records	30M < 60M Records	> 60M Records or Unknown			
		IO3: Criticality of the business relationship	None or N/A	Minimal	Low	Moderate	High	Critical, or unknown			
	Compliance	IC1: Comp. and specificity of requirements	None or N/A	Targeted, non-specific	General, non-specific	General framework	Prescriptive framework	Comprehensive framework or unknown	Simple Average		
		IC3: Specified or observed fines/ penalties	None or N/A	Insignificant	Minor	Moderate	Significant	Catastrophic or unknown			
		IC4: Level of enforcement	None or N/A	Inconsistent Ad Hoc	Reactive	Proactive, predictable	Proactive, unpredictable	Aggressive, or unknown			
Likelihood	Technical	LT1: Data processing/ storage environment	None or N/A	Private cloud	Hybrid cloud	Public cloud	Colo datacenter	On-premises or unknown	Simple Average		
		LT2: Type of equipment used	None or N/A	Org-provided virtual workspaces only	Org-managed virtual workspaces only	Org-owned/ leased workstations only	Includes personally owned workstations	Includes cell phones / tablets, or unknown			
		LT3: Data access approach	None or N/A	Onsite (Supervised)	Onsite (Unsupervised)	Offsite (No Remote access)	Remote access (Individual)	Remote access (Group), or unknown			
		LT4: Nature of Sys. Dev. / Maintenance	None or N/A	Minimal, internal function	Minimal, outsourced developers	Significant, internal function	Significant, outsourced developers	Uses offshore developers			
		LT5: Use of subcontractors	None or N/A	Single sub, domestic	Many subs, domestic	Single sub in another country	Many subs in another country	Many subs in many countries, or unknown			
		LT6: Location of permitted remote access	None or N/A	Corporate locations only, domestic	Corporate locations only, many countries	Workforce personnel residences	Public locations	High-risk countries			

A minimally viable implementation of the HITRUST TPRM Methodology would equate the inherent risk score with a corresponding level of assurance as determined by the Assurance Rely-Ability Maturity Model (ARMM).

Table 2. Assurance Rely-Ability Maturity Model

ARMM			Assessment Approach		
			Raw / Normalized Scores		
Dimension	**Attribute**	**Indicator**	**Indicator**	**Attribute**	**Dimension**
Suitability	Comprehensiveness	Basis of Control Selection			Simple Average
	Prescriptiveness	Specificity of the Controls			
	Accuracy	Context of the Control Requirements			
	Scalability	Flexibility of Control Selection		Simple Average	
		Reporting Options			
	Consistency	Consistency of Control Selection			
	Efficiency	Supports Multiple Frameworks			
	Transparency	Approach to Control Selection			
Impartiality	Comprehensiveness	N/A			Simple Average
	Prescriptiveness	Specificity of Requirement Performance			
	Accuracy	Approach to Scoring Maturity			
	Scalability	Scaling to Different Sizes/Types of Orgs			
	Consistency	Initial Control Selection		Simple Average	
		Quality Review for Internal Consistency			
		Quality Review for External Consistency			
	Efficiency	Availability of Mappings			
	Transparency	Availability of Requirements			
Rigor	Comprehensiveness	Approach to Evaluating Maturity			Simple Average
	Prescriptiveness	Assessment Approach/Procedures			
	Accuracy	Granularity of Measurement Scale			
	Consistency	Reporting Source		Simple Average	
		Assessor Vetting			
		Assessor Training Requirement			
		Assessor Training Source			
		Quality Review (Procedures / Deliverables)			
	Efficiency	Generalizability of the Report		Simple Average	
		Availability of the Report			
		Ease of Report Distribution			
	Transparency	Availability of the Scoring Approach			

Assurance Rely-Ability scores are computed 'quasi-quantitatively' by ranking features of an assurance approach relevant to various assurance indicators along a 5-point Fibonacci-based scale of 1, 2, 3, 5, 8, which are then aggregated as simple averages along each attribute and dimension. While an average can also be computed for an estimate of overall Rely-Ability of an assurance approach, HITRUST takes a more conservative 'low watermark' approach to expressing overall Rely-Ability by using the lowest scoring dimension of assurance and normalizing the value on a 100-point scale.

DEVELOPER TIP: Although a minimally viable implementation is based on the inherent risk score and the lowest-scoring dimension, HITRUST recommends implementing additional capability that would allow organizations to place constraints on the selection of an assurance method based on organization-defined minimum values of one or more indicators and/or attributes consistent with organizational risk tolerances.

$$Normalized\ Rely\text{-}ability\ Score = ROUND\left[\frac{Raw\ Rely\text{-}ability\ Score\ x\ 100}{8}\right]$$

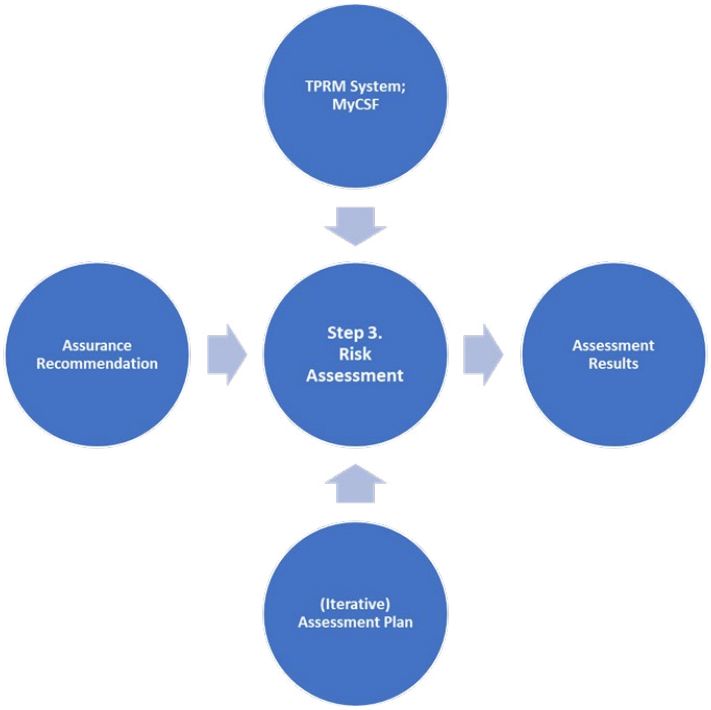
HITRUST determines the range of normalized Rely-Ability scores equivalent to a level of assurance using an academic grading model, which is an intuitive way to communicate performance to non-technical stakeholders, and also 'bounds' the category for minimal assurance between 0 and 12.5 to reflect how a raw Rely-Ability score of less than one on a scale of zero to eight would be rounded down to provide a 'zero' similar to the inherent risk approach. A complete mapping of inherent risk scores to levels of assurance is shown in Table 3 below.

Table 3. Levels of Assurance Commensurate with Inherent Risk

Inherent Risk Score	Inherent Risk	Level of Assurance	Rely-Ability Score
0	Negligible	Minimal	0 – 12.5
1	Very Low	Very Low	12.5 – 59
2	Low	Low	60 - 69
3	Moderate	Moderate	70 – 79
4	High	High	80 – 89
5	Very High	Very High	90 - 100

Qualify Step 3 – Risk Assessment

Figure 7. Qualify Step 3 – Risk Assessment



After the appropriate level of assurance is selected in the Risk Triage Process (Qualify Step 2 – Risk Triage), the TPRM analyst (or other responsible individual) should notify the third party, communicate acceptable approaches to providing the requisite assurances (i.e., a qualifying assessment), agree on a specific approach, establish a timeline for compliance, and monitor the third party's progress until the requisite assurances are provided.

Regardless of the approach selected, organizations should ensure the associated qualifying assessment addresses the following requirements or, if one or more interim assessments are provided as part of an iterative assurance process, ensure deficiencies are addressed in subsequent assessments:

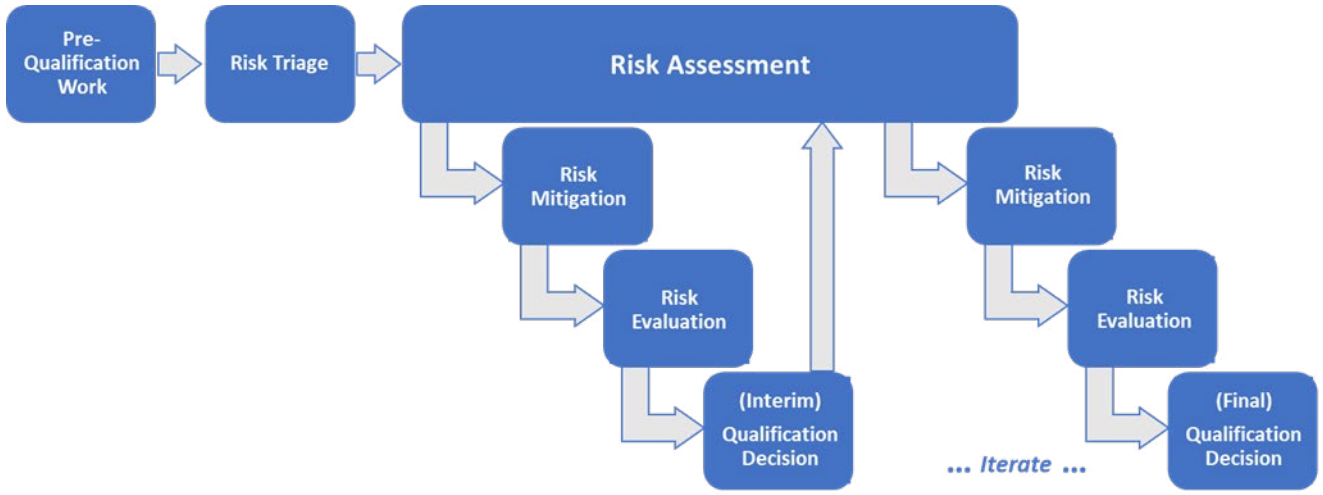
- The qualifying assessment is appropriate to the inherent risk of the business relationship, e.g., a very low level of assurance will not satisfy the assurance requirements for a moderate level of inherent risk,
- The qualifying assessment scope covers the scope required for the product(s) and/or services(s) provided or will be provided by the third party, i.e., no part of the organization and/or no system that must be addressed by the assessment are excluded,
- The qualifying assessment includes a complete specification of controls appropriate to the intended level of assurance, and
- The qualifying assessment does not include corrective action plans (CAPs) when CAPs are not allowed for an approach or contains more CAPs than would otherwise be allowed for the level of assurance required.

DEVELOPER TIP: Additional requirements such as those indicated here (e.g., the specific scope of the assessment) should be included in the TPRM system, communicated to the third party, and checked off in the system upon receipt of the qualifying assessment as part of an integrated workflow management capability.

If a qualifying assessment is acceptable, the 'gate' for the requisite level of assurance has been reached and the organization may proceed to Qualify Step 4 – Risk Mitigation. However, if the assessment provided by the third party does not satisfy any one of these requirements, the organization will need to work with the third party to ensure one or more additional assessments are performed to address any deficiencies.

If a third party is unable to provide the requisite level of assurance as requested, the organization can choose to accept interim levels of assurance until the third party is able to do so, as shown in Figure 8 below.

Figure 8. Iterative View of the TPRM Qualify Process



As an iterative progression, the organization should set milestones for delivery of each interim assessment until the final qualifying assessment with the requisite level of assurance is received.

DEVELOPER TIP: THE TPRM system's workflow management capability should have the ability to address the iterative nature of the qualification process.

DEVELOPER TIP: The system should also include the ability to send and receive information with the organization's third parties via standard messaging (e.g., email) or direct access (e.g., via an appropriate web interface) throughout the entire iterative third-party qualification process. A direct interface with external assessment repositories is also beneficial.

Although each qualifying assessment received in the risk assessment step is technically discrete, HITRUST views risk assessment as an ongoing activity, much like continuous monitoring, since a new assessment may begin almost as soon as an interim assessment is completed. Risk mitigation, risk evaluation, and the qualification decision however are considered discrete since they are essentially tied to a single assessment, and the completion of one step does not necessarily start another, e.g., another qualification decision is not initiated until after the next qualifying assessment is received, deficiencies are reviewed, and the corresponding risk is evaluated.

Qualify Step 4 – Risk Mitigation

Figure 9. Qualify Step 4 – Risk Mitigation

Although Step 4 – Risk Mitigation is technically a separate step in the qualification process, it should be initiated after the receipt of any assessment received by the organization from a third party as a matter of routine, whether as a final qualifying assessment or an interim assessment as part of an iterative assurance process (as shown by Figure 8 in the previous section). This is necessary as each qualifying assessment serves as a 'gate' during which the organization evaluates the level of anticipated residual risk due to any deficiencies (e.g., inadequate scope of assessment or gaps in control implementation) in Step 5 – Risk Evaluation, and determines if the third party may continue through the qualification process (if an interim assessment) or makes a final qualification decision in Step 6 – Qualification Recommendation.

If there are deficiencies, a complete Corrective Action Plan (CAP) should include, at a minimum, a control gap identifier, description of the control gap, CSF control mapping, point of contact, resources required (dollars, time, and/or personnel), scheduled completion date, corrective actions, how the weakness was identified (assessment, Assessor, date), date identified, and current status.

DEVELOPER TIP: The TPRM system should be capable of importing CAP information from structured assessment reports in addition to supporting manual entry of CAPs by a TPRM analyst. CAP fields should comport with HITRUST's minimum requirements for CAP information as well as have the ability to add organization-defined CAP entries. CAP entry and maintenance should also be included as part of the standard workflow management system.

As some assessment reports do not include information on CAPs for identified control deficiencies, the organization must work with the third party to ensure appropriate CAPs are developed and the actions taken will adequately address the gaps.

Once a gap is identified, a third party generally:

1. Assesses the gap between the current state and the intended (target) state of control implementation
2. Evaluates the potential consequences arising from the gap, such as the impact on other controls and the amount of excessive residual risk
3. Determines which gaps need to be mitigated and which can be accepted
4. Identifies actions to mitigate the gaps and document the actions in a CAP
5. Performs a cost-benefit analysis (CBA) or similar analysis on any potential risk reduction
6. Prioritizes the CAPs based on the results of the CBA or similar analysis and any potential consequences

DEVELOPER TIP: Although not required for a minimally viable TPRM system, HITRUST recommends incorporating the capability for third parties to develop and/or document CAPs within the system via a web interface or allow the data to be uploaded to the system based on a standard application programming interface (API).

Once CAPs are received from the third party, the organization must review them and ensure the actions and the timeline for their implementation are acceptable. If not, the organization will need to work with the third party to determine if any outstanding issues with the plan(s) can be addressed before proceeding to Qualify Step 5 – Risk Acceptance.

For those control requirements a third party may not wish to implement, the organization should work with the third party to identify one or more acceptable compensating controls to implement in their place. The organization should base approval on a valid risk analysis and document the analysis and approval in the TPRM system. (Alternative risk treatments are addressed in the next section.)

DEVELOPER TIP: A minimally viable TPRM system should be capable of documenting the substitution of a required control with one or more compensating controls along with the associated risk analysis and approvals by both the third party and the organization.

An organization can also take several approaches to managing CAPs during an iterative assessment process. For example, it can chose to:

- Identify and track 'key' or 'concerning' CAPs separately until the next qualifying assessment is received,
- Not identify and track 'key' or 'concerning' CAPs, but require the organization to resubmit the 'current' qualifying assessment report once 'key' or 'concerning' CAPs have been remediated, or
- Track CAPs separately from the assessment and wait until the next scheduled qualifying assessment is submitted to update CAP status.

Qualify Step 5 – Risk Evaluation

Figure 10. Qualify Step 5 – Risk Evaluation

Once an assessment has been received, whether provided as interim assurance or as the third party's final submission, the organization must evaluate the remaining residual risk and prepare a recommendation to the individual or office authorized to accept risk on behalf of the organization.

The remaining residual risk is an aggregate of the residual risk posed by each of the individual risk strategies adopted by the third party, i.e., through mitigation (as evidenced by control maturity scores, gaps in implementation, and related CAPs), transfer (e.g., indemnification and cyber insurance if relevant to the organization's risk rather than simply the third party's), avoidance (e.g., by changing the way they access and/or process information), or acceptance (e.g., by choosing not to mitigate, transfer, avoid a particular risk).

DEVELOPER TIP: In addition to parsing the maturity of implementation for each control requirement assessed, the TPRM system must be able to document the risk strategy employed for any control gaps, including the third-party's acceptance by an appropriate level of management, and the organization's own review and acceptance or rejection of the strategy with an appropriate rationale.

To evaluate residual risk, the HITRUST TPRM Methodology assumes that acceptable residual risk is defined by 100% implementation of the control requirements specified in the assessment. Whether a qualifying assessment is based on a subset of control requirements, such as those related to best practices, or is a complete specification based on an analysis of all relevant risks, the controls are deemed appropriate to the level of inherent risk incurred in a specific business relationship and subsequently the level of assurance required from the third party. For all intents and purposes, unacceptable residual risk is zero.

The simplest approach to computing the additional residual risk due to control noncompliance is to use control maturity as an estimate of the likelihood a control requirement will fail (i.e., a threat will exploit one or more vulnerabilities addressed by the requirement) and HITRUST CSF control impact codes as an estimate of the relative impact to the organization relative to other control requirements.

Table 4. HITRUST CSF Control Impact Codes

Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code
0.a	3	01.o	3	02.e	5	05.e	3	06.i	4	08.i	4	09.k	3	09.z	5	10.i	4
01.a	5	01.p	3	02.f	5	05.f	4	06.j	3	08.j	4	09.l	3	09.aa	3	10.j	4
01.b	5	01.q	5	02.g	5	05.g	4	07.a	4	08.k	5	09.m	4	09.ab	3	10.k	4
01.c	5	01.r	4	02.h	5	05.h	5	07.b	3	08.l	5	09.n	4	09.ac	3	10.l	3
01.d	5	01.s	4	02.i	5	05.i	4	07.c	5	08.m	5	09.o	3	09.ad	3	10.m	3
01.e	5	01.t	3	03.a	3	05.j	5	07.d	4	09.a	5	09.p	5	09.ae	3	11.a	3
01.f	5	01.u	3	03.b	3	05.k	5	07.e	5	09.b	4	09.q	4	09.af	3	11.b	4
01.g	4	01.v	3	03.c	3	06.a	4	08.a	5	09.c	5	09.r	4	10.a	4	11.c	3
01.h	3	01.w	3	03.d	3	06.b	4	08.b	5	09.d	4	09.s	5	10.b	4	11.d	3
01.i	4	01.x	5	04.a	3	06.c	3	08.c	5	09.e	4	09.t	3	10.c	4	11.e	3
01.j	5	01.y	5	04.b	3	06.d	3	08.d	4	09.f	4	09.u	3	10.d	3	12.a	3
01.k	4	02.a	4	05.a	4	06.e	5	08.e	5	09.g	4	09.v	4	10.e	4	12.b	3
01.l	4	02.b	5	05.b	5	06.f	4	08.f	4	09.h	3	09.w	4	10.f	3	12.c	3
01.m	3	02.c	5	05.c	3	06.g	4	08.g	4	09.i	4	09.x	4	10.g	3	12.d	3
01.n	4	02.d	4	05.d	3	06.h	4	08.h	3	09.j	4	09.y	4	10.h	4	12.e	3

Additional residual risk, ΔR, may then be computed as:

$$\Delta R = \frac{\sum L \times I}{\sum I} \times 100$$

L is the likelihood of a control failure, which is evaluated as one minus the assessed maturity of a control requirement's implementation, and I is the impact code.

Additional residual risk is essentially a quasi-quantitative measure based on the likelihood of individual control failures weighted by the relative impact of those failures. As the likelihood of a control failure goes to zero, the additional residual risk also goes to zero. However, as likelihood approaches one, the additional residual risk approaches one hundred.

When using this approach to evaluating additional residual risk, scores may be aggregated across HITRUST CSF controls, control objectives, and control categories; or topical/targeted groupings of control requirements (e.g., wireless networks and devices). It is subsequently useful to communicate these risks in the same manner.

To do so, HITRUST recommends the use of one of two types of risk scales: a 'traditional' bell-shaped or 'Gaussian' model and a left-skewed bell-shaped 'academic' model.

DEVELOPER TIP: While a minimally viable TPRM system will incorporate this approach to evaluating additional residual risk, HITRUST recommends the system also provide the capability to implement organization-defined values of likelihood and impact, e.g., using HITRUST's patent-pending approach to quasi-quantitative residual risk analysis (QQRRA).

Table 5. Gaussian and Academic Risk Scales

Risk Level	Range	
	Gaussian Model	Academic Model
Very High (Severe)	96-100	41-100
High	80-95	31-40
Moderate	21-79	21-30
Low	5-20	11-20
Very Low (Minimal)	0-4	0-10

Although the Gaussian model is widely used, the academic model provides an intuitive approach to understanding risk when presented as risk grades, which is similar to the model used by the U.S. federal government in the past to report security compliance by federal agencies.

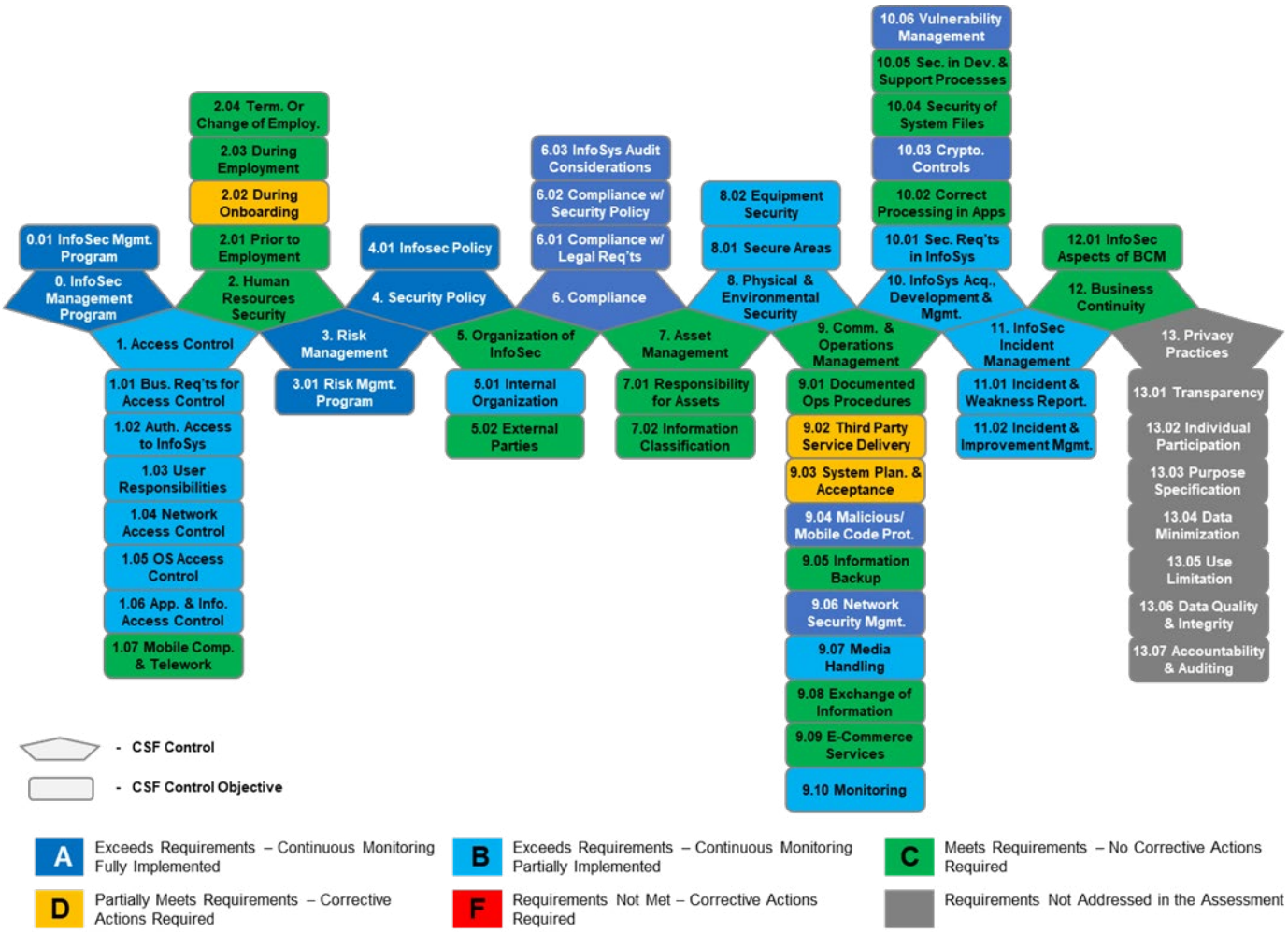
Risk grades may be computed from the academic risk scores by subtracting them from 100 and using a traditional academic grading scale: A (90-100), B (80-89), C (70-79), D (60-69) and F (0-59). The grades basically let management know how well they are managing residual risk due to "immature" controls in the environment.

In the context of a HITRUST r2 Assessment that uses a 5-level maturity model, full implementation of a control, i.e., full credit for the policy, procedures, and implementation (and optionally managed and measured) maturity levels, would generally provide an overall "C" for the organization, which would be considered average for the industry. Organizations receive higher grades (an "A" or "B") through continuous monitoring (measurement) and active management of control effectiveness. The figure on the following page provides an example of what an academic 'scorecard' might look like for a HITRUST r2 Assessment with risk aggregated by control objective.

When using QQRRA or a similar approach to calculating quasi-quantitative monetary estimates of loss and the application of control attributes to the risk calculus, the information can also be displayed based on specific risks, areas of risk, and—of course—the business relationships evaluated using the TPRM Methodology. In this case, specific numeric values or ranges of values should always be used regardless of whether the information is displayed graphically or in a tabular form.

DEVELOPER TIP: HITRUST recommends implementation of multiple approaches to dashboarding third party compliance and/or risk in the TPRM system. In addition to the scales and dashboards discussed here, developers should include the ability for organizations to design their own dashboards based on organization-defined criteria for aggregating control scores and/or risk scores as well as the specific scales used in categorizing controls and/or risk scores.

Figure 11. Example of Academic Risk Scorecard (HITRUST CSF)



Qualify Step 6 – Qualification Decision

Figure 12. Qualify Step 6 – Qualification Decision

Once excessive residual risk has been evaluated, the TPRM analyst will compile information from the assessment report(s), generate any additional information, e.g., various risk scorecards to address specific areas of interest or concern, and include a recommendation for or against risk acceptance by the organization based on a comparative analysis of the assessment results with the required assurance level specified in Qualify Step 3 – Risk Triage as well as any additional criteria established by the organization, e.g., minimum control maturity scores. A formal qualification decision is made by TPRM leadership in Step 6 – Qualification Decision based on the TPRM analyst's risk acceptance recommendation and supporting documentation, which either qualifies a third party to continue an iterative assessment process and/or begin (or continue) doing business based on the remaining residual risk to the organization.

As indicated earlier in Figure 8, risk recommendations and related qualification decisions are 'baked' into the process with the receipt of every qualifying assessment until the final qualifying assessment is provided. However, a new risk recommendation and/or qualification decision may be issued between the receipt of a qualifying assessment based on in-flight tracking of a third party's progress against (1) established qualifying assessment milestones, e.g., the next assessment is overdue, and (2) remediation of control deficiencies based on associated CAPs in the most current assessment, e.g., a lack of progress in remediating a deficiency indicates it will not be successfully addressed, either with an agreed timeline or scope of implementation.

DEVELOPER TIP: The TPRM system should be capable of tracking established milestones for the receipt of assessments as well as progress with the remediation of identified control deficiencies (i.e., CAPs) against established deadlines. The system should also alert the responsible TPRM analysis whenever a particular milestone/deadline is missed.

Although the risk acceptance decision is formally addressed in TPRM Step 4 – Accept, it's important to note that an organization's decision-maker should be allowed to escalate a risk acceptance recommendation to executive management, an enterprise risk management board, or even a board of directors under specific circumstances, e.g., when there is significant stakeholder interest or concern about the proposed business relationship and the organization's level of risk tolerance is exceeded or close to being exceeded. HITRUST recommends organizations identify conditions for escalation in advance as part of their formal TPRM program.

It may also be beneficial to provide a similar escalation path for staff preparing the risk acceptance recommendation to help ensure proper alignment with the organization's business strategy and objectives.

DEVELOPER TIP: The TPRM system should incorporate all elements of the risk recommendation evaluation, decision, and escalation workflows, which may also require interfacing with organizational messaging, procurement, contracting, and/or other related systems, as required.

Leveraging HITRUST Products and Services

There are many components and considerations in developing and implementing a robust organizational TPRM program that encompasses and integrates all the elements needed to manage third party risk and achieve one's compliance objectives effectively. Many organizations believe selecting an information risk management framework is the most complicated part of the process, and although important, it is just the beginning.

HITRUST champions programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. We develop, maintain, and provide broad access to widely adopted common risk and compliance management frameworks and related assessment and assurance methodologies. Our comprehensive suite of products, services, and tools provide an integrated approach to aligning, maintaining, and supporting an organization's information third-party risk management program and meet the challenges of managing tens, hundreds, thousands or more vendors, suppliers, and other third parties.

HITRUST brings Rely-Ability and efficiency to all levels of information assurance by offering unique, industry-leading benefits to both organizations and their third parties.

- Uses single HITRUST CSF framework, which harmonizes multiple standards and authoritative sources.
- Leverages a common assurance methodology.
- Provides granular control requirements for added specificity.
- Relies on best-in-class HITRUST MyCSF® SaaS assessment platform to share data between assessed entities, external assessors, and the HITRUST Quality Assurance team.
- Allows internal and external inheritance from previously completed HITRUST assessments.
- Shares assessment results with relying parties electronically and securely through the HITRUST Results Distribution System (RDS).
- Utilizes the HITRUST Assurance Intelligence Engine (AIE) for greater reliability and accuracy.

The HITRUST Assessment Portfolio is uniquely suited for TPRM by offering three different types of assessment that are specifically designed to build upon one another in terms of the controls required for assessment and the impartiality and rigor of their assessment and subsequently address the complete range of inherent risk third parties may present:

- **HITRUST Basic, 1-year (b1) Validated Assessment + Certification.** The b1 offers a "good hygiene" assessment suitable for third parties that present a low level of inherent risk to an organization but still offers higher reliability than other self-assessments and questionnaires by utilizing the HITRUST Assurance Intelligence Engine (AI Engine) to identify errors and omissions. A HITRUST b1 Readiness Assessment is also available.
- **HITRUST Implemented, 1-Year (i1) Validated Assessment + Certification.** The i1 is a "best practices" assessment recommended for situations that present moderate risk. The i1 is a new-class of information security assessment that is threat-adaptive with a control set that evolves over time to deliver continuous cyber relevance. The i1 is designed to keep pace with the latest cyberattack threats, including ransomware and phishing. A HITRUST i1 Readiness Assessment is also available.
- **HITRUST Risk-based, 2-Year (r2) Validated Assessment + Certification.** Formerly named the HITRUST CSF Validated Assessment, the r2 remains the industry gold standard as a risk-based and tailorable assessment that continues to provide the highest level of assurance for situations with greater risk exposure due to data volumes, regulatory compliance, or other risk factors. HITRUST r2 Readiness, Interim, and Bridge Assessments are also available.

Table 6 below provides the lowest scoring dimension of Rely-Ability for each of the four general types of assessment in the HITRUST Assessment Portfolio and how they relate to each category of inherent risk computed during Step 2 – Risk Triage.

Table 6. HITRUST Assessment Portfolio Rely-Ability Scores

Inherent Risk Score	Inherent Risk	Level of Assurance	Rely-Ability Range	HITRUST Assessment	Rely-Ability Score (Low Watermark)	Minimum Risk Requirements
0	Negligible	Minimal	0 – 12.5	N/A	0	N/A
1	Very Low	Very Low	12.5 - 59	b1 Readiness	56.4	None
2	Low	Low	60 – 69	b1	69.6	Cert/No CAPs
3	Moderate	Moderate	70 – 79	i1	71.5	CAPs Allowed
4	High	High	80 – 89	r2	93.8	CAPs Allowed
5	Very High	Very High	90-100	r2	93.8	Cert/No CAPs

The raw scores for each assurance reliability indicator, attribute, and dimension are provided in Table 7 on the following page.

The HITRUST b1 Readiness, b1, i1, and r2 Assessments fit neatly in the very low, low, moderate, and very high assurance categories; the r2 is also recommended for the high assurance category as well. This is because HITRUST believes high and very high levels of assurance require an assessment of a risk-based specification of controls in order to gain a better understanding of how a third party is addressing all reasonably anticipated threats (and subsequently risks) to the information it accesses and processes on behalf of a relying party. And, although the Rely-Ability scores for the r2 Assessment and r2 Assessment with Certification and no CAPs are the same (i.e., both provide the same level of trustworthiness in the information they provide), the latter provides minimum requirements for control implementation that help ensure any additional residual risk to the organization is similarly minimal.

As some HITRUST Assessment Reports do not come with CAPs, the organization will need to work with the third party to ensure appropriate CAPs are developed and the actions taken will adequately address the gaps. However, all HITRUST r2 Assessment Reports that are not Certified come with required CAPs to address gaps that prevent it from meeting the minimum requirements for certification, and all r2 Assessment Reports that meet the requirements for HITRUST Certification will come with required CAPs for similar reasons; however, the third party must typically address those requirements before it can recertify.

While HITRUST does not generally recommend the use of self-assessments for third-party assurance, we have always posited they are acceptable when a third party presents a very low risk to a relying party. We subsequently recommend the use of a b1 Readiness Assessment for very low inherent risk/assurance requirements but specifically do not recommend an i1 or r2 Readiness Assessment as the final qualifying assessment for higher levels of assurance. However, we do recommend organizations consider Readiness Assessments as part of an iterative approach to obtaining the final qualifying assessment required.

To illustrate this approach, we provide a few examples following the next table that are based on recommended timelines for the achievement of each assessment in the HITRUST Assessment Portfolio.

Table 7. Assurance Scores for Assessments in the HITRUST Portfolio

ARMM			Assurance (Assessment) Approach																			
			Indicator Scores				Attribute Scores				Dimension Scores				Rely-Ability Scores (Low Watermark)				Normalized Scores (Low Watermark)			
Dimension	**Attribute**	**Indicator**	**b1R**	**b1**	**i1**	**r2**	**b1R**	**b1**	**i1**	**r2**	**b1R**	**b1**	**i1**	**r2**	**b1R**	**b1**	**i1**	**r2**	**b1R**	**b1**	**i1**	**r2**
Suitability	Comprehensiveness	Basis of Control Selection	3	3	5	8	3.0	3.0	5.0	8.0	5.6	5.6	5.9	8.0	4.5	5.6	5.7	7.5	56.4	69.6	71.5	93.8
	Prescriptiveness	Specificity of the Controls	8	8	8	8	8.0	8.0	8.0	8.0												
	Accuracy	Context of the Control Requirements	8	8	8	8	8.0	8.0	8.0	8.0												
	Scalability	Flexibility of Control Selection	1	1	1	8	1.0	1.0	1.0	8.0												
		Reporting Options	1	1	8	8																
	Consistency	Consistency of Control Selection	8	8	8	8	8.0	8.0	8.0	8.0												
	Efficiency	Supports Multiple Frameworks	8	8	8	8	8.0	8.0	8.0	8.0												
	Transparency	Approach to Control Selection	3	3	3	8	3.0	3.0	3.0	8.0												
Impartiality	Comprehensiveness	N/A	-	-	-	-	-	-	-	-	5.9	6.7	7.5	7.5								
	Prescriptiveness	Specificity of Requirement Performance	3	3	8	8	3.0	3.0	8.0	8.0												
	Accuracy	Approach to Scoring Maturity	8	8	8	8	8.0	8.0	8.0	8.0												
	Scalability	Scaling to Different Sizes/Types of Orgs	8	8	8	8	8.0	3.0	8.0	8.0												
	Consistency	Initial Control Selection	8	8	8	8	3.3	8.0	8.0	8.0												
		Quality Review for Internal Consistency	1	8	8	8																
		Quality Review for External Consistency	1	8	8	8																
	Efficiency	Availability of Mappings	8	8	8	8	8.0	8.0	8.0	8.0												
	Transparency	Availability of Requirements	5	5	5	5	5.0	5.0	5.0	5.0												
Rigor	Comprehensiveness	Approach to Evaluating Maturity	1	1	1	8	1.0	1.0	1.0	8.0	4.5	5.7	5.7	8.0								
	Prescriptiveness	Assessment Approach/Procedures	8	8	8	8	8.0	8.0	8.0	8.0												
	Accuracy	Granularity of Measurement Scale	8	8	8	8	8.0	8.0	8.0	8.0												
	Consistency	Reporting Source	8	8	8	8	2.4	8.0	8.0	8.0												
		Assessor Vetting	1	8	8	8																
		Assessor Training Requirement	1	8	8	8																
		Assessor Training Source	1	8	8	8																
		Quality Review (Procedures / Deliverables)	1	8	8	8																
	Efficiency	Generalizability of the Report	3	3	3	8	4.7	6.3	6.3	8.0												
		Availability of the Report	8	8	8	8																
		Ease of Report Distribution	3	8	8	8																
	Transparency	Availability of the Scoring Approach	8	8	8	8	8.0	8.0	8.0	8.0												

Table 8 provides a low and high estimate for each assessment based on our experience working with assessors and assessed organizations; however, organizations should adjust these values based on relevant factors such as any existing assessment reports a third party can provide or their perceptions around the state of their information protection programs.

Table 8. HITRUST Assessment Portfolio Assessment Timelines

HITRUST Assessment	Minimum Expected Time	Maximum Expected Time
b1 Readiness	2 weeks	4 weeks
b1	1 month	4 months
i1 Readiness	3 months	6 months
i1	6 months	9 months
r2 Readiness	3 months	6 months
r2	12 months	18 months

Scenario 1

A third party has a very robust information protection program that has undergone third party assessment against the NIST SP 800-53 moderate impact baseline due to their status as a federal contractor. They present a high level of inherent risk, and the organization agrees to an interim assessment approach with the potential to award a contract based on the results of the first assessment.

Table 9. Scenario 1 Milestones/Timeline

HITRUST Assessment	Type of Qualifying Assessment	Time Allotted	Milestones/Timeline
r2 Readiness	Interim	3 months	3 months
r2	Final	12 months	15 months

Scenario 2

A third party has an information protection program based on security management's perception of best practices rather than a generally accepted control framework like the HITRUST CSF. They present a moderate amount of inherent risk for a proposed business relationship, and the organization agrees to an interim assessment approach as long as they receive the final qualifying assessment before contract award at the beginning of the fiscal year in 6 months.

Table 10. Scenario 2 Milestones/Timeline

HITRUST Assessment	Type of Qualifying Assessment	Time Allotted	Milestone/Timeline
b1 Readiness	Interim	2 weeks	2 weeks
i1 Readiness	Interim	2-1/2 months	3 months
i1	Final	3 months	6 months

Closing Thoughts

The heart of a successful TPRM program is the HITRUST TPRM Qualification Methodology, which provides organizations with a comprehensive approach to manage their third-party risk consistently, efficiently, and effectively at a reasonable cost by:

- Defining inherent risk factors,
- Triaging third parties based on inherent risk,
- Evaluating, and reporting on residual risk, and
- Qualifying third parties for business by making a formal recommendation for the acceptance of that risk.

Widespread adoption provides similar benefits for third parties by allowing them to leverage their TPRM-based assessments for multiple customer organizations: a 'win-win' for organizations and third parties alike.

However, organizations should ensure the methodology is implemented faithfully, i.e., in such a way as to ensure organizational TPRM programs provide a minimum standard of care acceptable to their stakeholders, including regulators, and the industry at large. They can do so by ensuring (1) leadership fully supports and provides adequate oversight of the implementation of the methodology as described in this handbook, (2) planning is adequate to the task, (3) steps are taken to improve the organization's culture with respect to organizational change in general and improving TPRM in particular, and (4) sufficient resources and training are made available to the workforce to ensure acceptance and routine use of the new TPRM requirements and processes.

About the Author

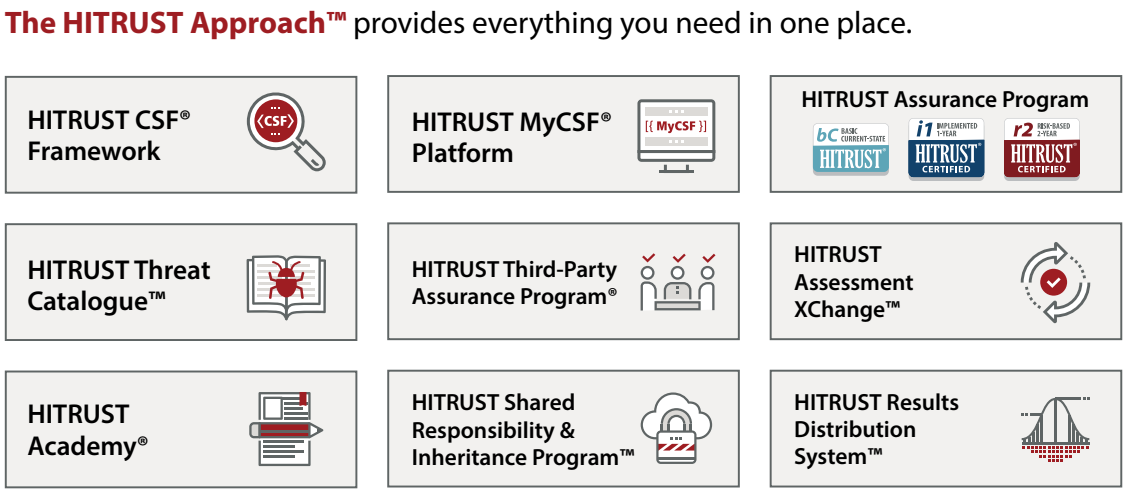
Bryan Cline, Ph.D., Chief Research Officer, HITRUST

Bryan provides thought leadership on risk management and compliance and develops the methodologies used in various components of the HITRUST Approach. This includes a focus on the design of the HITRUST CSF and the assessment and certification models used in the HITRUST Assurance Program, for which he provides technical direction and oversight. He is also responsible for addressing emerging trends impacting risk management and compliance to ensure the HITRUST Approach sets the bar for organizations seeking the most comprehensive privacy and security frameworks available. Bryan previously served as HITRUST's Vice President of Standards and Analysis.

About HITRUST

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks, as well as related assessments and assurance methodologies.

Figure 13. The HITRUST Approach



HITRUST also actively participates in many efforts in government advocacy, community building, and cybersecurity education. For more information, visit www.hitrustalliance.net.

Bibliography

Bennekers, V. (Ed.) (2022). HITRUST Assessment Handbook. Frisco, TX: HITRUST.

Bowen, P. and Kissel, R. (2007, Jan). Program Review for Information Security Management Assistance (PRISMA) (NISTIR 7358). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7358.pdf.

Cline, B. (2008). Factors Related to the Implementation of Information Systems Security Engineering: A Quality Perspective. [Doctoral dissertation, University of Fairfax].

Cline, B. (2022a). Quantifying Risk in a Qualitative World: The HITRUST Approach to Quasi-Quantitative Residual Risk Analysis (QQRRA). Frisco, TX: HITRUST.

Cline, B. (2022, Jul). HITRUST Third-Party Risk Management (TPRM) Methodology: The Qualification Process – A streamlined approach to qualifying a third party for a business relationship leveraging the HITRUST CSF and Assurance Program, Version 2.1. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/uploads/TPRM-Methodology1.pdf.

Cline, B. (2022). The HITRUST Risk Management Handbook: A discussion of framework-based risk analysis and control specification, implementation, assessment, and reporting for HITRUST Organizations and Assessors. Frisco, TX: HITRUST.

Cornell Law School (2021, Sep). Standard of Care. In Legal Information Institute law dictionary. Available from https://www.law.cornell.edu/wex/standard_of_care.

HITRUST (2022a). About HITRUST. Available from https://hitrustalliance.net/about-hitrust/.

HITRUST (2022b). HITRUST CSF. Available from https://hitrustalliance.net/hitrust-csf/.

HITRUST (2022c). HITRUST Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/.

HITRUST (2022d). HITRUST Approach. Available from https://hitrustalliance.net/the-hitrust-approach/.

HITRUST (2022e). HITRUST Implemented, 1-Year (i1) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-implemented-1-year-i1-validated-assessment/.

HITRUST (2022f). HITRUST Risk-based, 2-Year (r2) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-risk-based-2-year-r2-validated-assessment/.

Joint HPH Cybersecurity WG (2016, May). Healthcare Sector Cybersecurity Framework Implementation Guide. Available from https://hitrustalliance.net/uploads/HPHCyberImplementationGuide.pdf.

Merriam-Webster (2022a). Standard of Care. In Merriam-Webster.com legal dictionary. Available from https://www.merriam-webster.com/legal/standard%20of%20care.

Merriam-Webster (2022b). Due Care. In Merriam-Webster.com legal dictionary. Available from https://www.merriam-webster.com/legal/due%20care.

Merriam-Webster (2022c). Due Care. In Merriam-Webster.com legal dictionary. Available from https://www.merriam-webster.com/legal/due%20care.

NIST (2018, 16 Apr). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Author. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

HITRUST®

FOR MORE INFORMATION:

Contact your HITRUST Product Specialist

Call: 855-448-7878 or Email: sales@hitrustalliance.net

www.hitrustalliance.net