

HITRUST



TPRM Implementation: Quick-Start Guide

Using a consistent, quantifiable six-step information risk triage assessment selection approach to establish healthy third-party business relationships

Introduction

Today's vendor ecosystems are rapidly growing, and as they continue to grow in size and complexity, the industry's challenges with third-party risk management (TPRM) continue to intensify.

For most organizations, a large and complex vendor ecosystem results in an uneven and incomplete understanding of risk, with no relationship between risk assessments, assurance mechanisms, and the inherent risk of each vendor relationship. This uneven understanding is especially problematic when a duty of care is involved.

What organizations need now is an actionable and appropriate way to qualify (and requalify) their vendors for business using a combination of standardized assessments and assurance mechanisms—one that is tightly aligned with an understanding of inherent risk.

Who should keep reading?

This guide is for anyone who is directly or indirectly involved in evaluating or managing the information security risk of third-party vendors to ensure suitability for doing business.

Whether you're a decision maker leading your organization's third-party risk program, an individual contributor who is in the trenches completing vendor risk assessments, or a cross-functional business owner who is anxious to get a third-party integrated into the business, read on. This guide has something for you.

What we'll cover

In this guide, we'll discuss how to:

- 1 Overcome key industry challenges related to third-party risk management.
- 2 Qualify vendors and suppliers based on their inherent level of risk.
- 3 Select and apply high-quality information security risk assessments to get more comfort and assurance.
- 4 Take a journey using one framework with consistent and common controls, and a standardized assurance program.
- 5 Harness the HITRUST portfolio appropriately for all tiers of vendor risk.

The journey is just getting started...

Inconsistent practices, critical pitfalls, and the need for more

Organizations vary quite a bit in their approach to third-party risk management, but they are unanimous on one thing: current vendor risk management approaches are broken. Let's look at some of TPRM's most critical shortcomings, and how we can build a bridge to a better way forward.



Unsustainable approaches.

The vendor ecosystem keeps growing, but the resource-intensive workflows of TPRM simply aren't sustainable—not for clients, not for vendors, not for anyone.



Lack of resources.

Internal teams are log-jammed as the scale of assessments continues to eclipse the capacity of internal resources. The result? Inevitable oversights that let risk creep in.



Limited remediation.

While the ecosystem continues to focus on assessments, little is being done to enforce the remediation of identified gaps.



Blind spots.

Many organizations have an incomplete understanding of risk, with a lot of data on a small portion of vendors and no data on all of the others. In addition, they have no actionable way to scan through thousands of assessments and surface vendors that have a critical threat control missing.



Outsized costs.

TPRM consumes significant financial and operational resources for internal teams, technologies, assurances, and so much more.



Long turnaround time.

Both assessments and assurances can be time-consuming, causing dissatisfied business stakeholders and slow contracting cycles.



Overwhelmed vendors.

Vendors are equally overwhelmed, and some even feel that exhaustive TPRM requirements outweigh the benefits of the contract itself.



High variance.

Organizations and risk leaders each have their own approach to TPRM, with no gold standard to guide the entire industry.



Insufficient assurance.

While validated third-party assurances are extremely valuable, many organizations have still not adopted them or are unsure where to start.

Relevant Resource


TPRM is Broken: Healthcare's Unsustainable Approach to Third-Party Vendor Risk Management

[READ THE BLOG](#)


Where do we go from here?

TPRM pitfalls are plentiful, and they can make the problem of vendor risk feel confusing and directionless at times. By aligning on some key tenets of success, we can find a better way forward for TPRM.

We believe that TPRM programs should provide standardized, efficient, and cost-effective evaluation and reduction of vendor and supply chain risks. To do this, we must:




Create norms around inherent risk and vendor tiering in the TPRM ecosystem.




Unlock the value of inherited trust through rigorous third-party assurance mechanisms.



Embrace healthy security program indicators and focus on cyber resiliency industry-wide.



Focus on understanding some risks for all vendors as opposed to all risk for a select few.



Drive constant security improvement through monitoring and remediation.

An actionable methodology for risk qualification

Qualifying vendors can be confusing, but it doesn't have to be. By consistently applying a well-defined process, organizations can more efficiently and effectively qualify (or requalify) third parties by obtaining assurances that are appropriate to the information security, privacy, and compliance risk they inherently pose to the organization.

Following is a six-step process that organizations can use for vendors of unknown risk and any new vendor relationships that are actively being considered for the organization.

Unknown Risk Vendor Population Includes existing vendors of unknown risk and new vendors the organization has not worked with before.



Step 1 Third-Party Pre-Qualification

- Engage with internal departments and external stakeholders.
- Review vendor data access and data processing.
- Assess the potential impact of the product and/or service on the organization.



Step 2 Risk Triage

- Evaluate the third party based on specific risk factors.
- Classify or tier the third party based on inherent risk.
- Determine the type of risk assessment needed to provide appropriate assurance.



Step 3 Risk Assessment

- Assess conformity to organization-defined security and privacy requirements.
- Obtain and review assurances.



Step 4 Risk Mitigation

- Evaluate gaps in conformity.
- Evaluate third-party corrective action plans (CAPs).
- Implement required CAPs to reduce risk to an acceptable level.



Step 5 Risk Evaluation

- Evaluate remaining residual risk.
- Prepare a qualification recommendation that aligns with organizational risk strategies.



Step 6 Third-Party Qualification

- Evaluate decision based on organizational risk appetite and specific risk tolerances.
- Engage management to make the final decision.
- Accept or reject the known third-party risk.



Continual Risk Monitoring

- Monitor potential changes in business risk.
- Consider information, security, and compliance forms of risk.
- Surface continuous insight to appropriate stakeholders.

Here are some of the reasons this qualification process works.



It is transparent, reliable, and well-accepted in the industry.



It is contextual, matching vendor risk with a minimum required assurance.



It is flexible, allowing organizations to accept more or less risk based on their tolerance.



It is practical, providing vendors a pathway to successive assurances and incremental improvements.

Mapping risk to assurance using the HITRUST Risk Triage

Third-party assurances have the power to radically improve organizational confidence in vendor security while also improving the overall efficiency of the third-party risk management process.

However, third-party assurances, particularly those that are most stringent, can require significant time, effort, and resource on the part of the vendor. For the organization, this can result in delayed contracting with a given vendor and—in some cases—the inability to work with a specific vendor altogether.

By mapping a vendor's inherent risk to the appropriate level of assurance, organizations and their third-parties can access the outsized benefits of third-party assurances while optimizing and balancing the complex relationship between risks, resources, and time. Enter the HITRUST Risk Triage.

For healthcare, this concept is not a new one. In fact, the triage process is a standard care practice that matches hospital patients to the level of care that is most appropriate to their need. Similarly, the HITRUST Risk Triage maps vendors to the most appropriate level of assurance.

Let's take a closer look at the HITRUST Risk Triage Model.



Evaluate **inherent risk**.



Map inherent risk to assurance level.



Select the **appropriate assurance**.





Evaluate inherent risk

Much like a medical triage, which begins with a careful evaluation of patient needs, the HITRUST Risk Triage begins with a careful evaluation of a vendor's level of inherent risk.

Inherent risk can be calculated using a combination of impact factors, which include the size of the potential business consequences, such as the nature and amount of data being handled and the degree to which compliance is involved; as well as likelihood of event-occurring factors, such as the nature of data processing and the use of subcontractors. Each of these risk factors is rated on a scale of 0 to 5, with 0 representing no risk and 5 representing very high risk.



Key Definitions

Risk Factors: A variable that makes a vendor more or less risky for the organization.

Impact: To what degree would a compromise impact the organization?

Likelihood: How likely is a compromise to happen?

What about missing data?

In reality, it is possible and even probable that some of the risk factors detailed above will require data that are either resource-intensive to acquire or missing altogether. In these cases, there are two potential approaches an organization can take.

The most **risk adverse approach** would be to assume the highest risk score for that element ($5/12 = 0.41$). This, on its own, is not capable of moving an organization out of its assigned inherent risk tier. An alternative approach would be to ignore the missing piece of data altogether as the model itself naturally balances various impacts with the likelihood of occurrence.

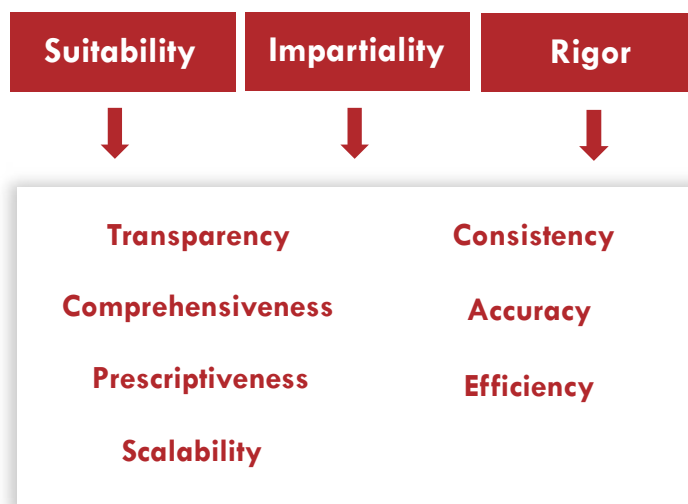


Map inherent risk to assurance level

Just as patients in a hospital do not all present the same level of severity, not all vendors present the same level of risk. Similarly, just as not all patients require the same level of care, not all vendors require the same level of assurance. Once inherent risk has been computed, the next step is to determine the appropriate level of assurance necessary to mitigate that risk.

Determining the appropriate level of assurance enables the organization to reserve its most rigorous requirements for those vendors that represent outsized risk while still achieving some assurance for vendors of medium or low risk levels. For vendors, this provides room to take a progressive approach to assurance that satisfies minimum requirements today so that a working relationship can commence while prioritizing greater levels of assurance (as needed) in the future. By using the HITRUST Assurance Rely-Ability™ Maturity Model (ARMM), organizations can evaluate and score assurances based on seven key attributes for each dimension of assurance quality, which include suitability, impartiality, and rigor.

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





Select the appropriate assurance

With an understanding of the appropriate assurance level for each vendor, organizations can then progress to assigning specific assurance requirements on a vendor-by-vendor basis. Generally speaking, the more rigorous a level of assurance, the more suitable and reliable the approach.

For vendors that pose only low inherent risk and require lower levels of assurance, a reliable self-assessment is typically suitable to affirm “good hygiene” and surface any errors. Organizations with higher levels of inherent risk and required assurance, however, require a much more robust, in-depth assessment and certification process to cover every risk factor. Example below:

Inherent Risk Score	Inherent Risk	Required Level of Assurance/ Score Range	HITRUST Assessment / Score
0	Negligible	Minimal 0-12.5	N/A
1	Very Low	Very Low 12.5-59	e1 Readiness 56.4
2	Low	Low 60-69	e1 Cert/ No CAPs 69.6
3	Moderate	Moderate 70-79	i1 CAPs Allowed 71.5
4	High	High 80-89	r2 CAPs Allowed 93.8
5	Very High	Very High 90-100	r2 Cert/ No CAPs 93.8

What about vendor push back?

As a practical matter, organizations looking to adopt the HITRUST Risk Triage approach will need to deal with vendor push back and are sure to hear the following:

- This is too high a level of effort or too much to ask.
- We’ve been a vendor for many years and you have never asked this of us before.
- No one else is asking me for this level of assurance.
- There isn’t enough time to get to the level you are asking of us.
- This vendor is too important to us; we can’t live without them. (From business stakeholders.)

To deal with these objections while driving for lower vendor risk, it is critical that the approach allows for time to achieve the targeted assurance level and visibility into the process so the organization can see milestones along the way. Plus, including efficiencies in the process make investments in incremental steps towards the targeted assurance progressive and fully reusable for the vendor.

Why validated assurances matter (but are not all created the same)

Third-party assurances are a powerful way to lift the burden of the TPRM process for everyone involved. In addition to providing greater assurance and validation than questionnaire-based processes, third-party assurances also foster greater standardization across the industry—both for vendors and the organizations they serve.



Greater **security assurance and validation**



Shift the burden **away from TPRM teams**



Foster **industry-wide standardization**



Assess once and provide assurance to many

But just because a third-party assurance exists doesn't mean it is reliable. In fact, different assessment reports can vary significantly in transparency, accuracy, consistency, and integrity, greatly impacting their suitability. Use these four pillars of RELY-ABILITY included in the HITRUST Approach to measure the suitability of the assurances your vendors are providing.

TRANSPARENCY

Transparency is needed for internal and external stakeholders to understand the framework your organization uses to satisfy core risk and compliance objectives. The framework should be publicly available, widely adopted, and well-understood so that report recipients understand how the controls were selected, evaluated, and scored.

Key Questions:

- Where do the assessed controls come from?
- How do you know the control requirements are suitable?

ACCURACY

Many other frameworks and assurance programs are qualitative, judgement-based, and devoid of any quantitative measurements. Assessment results should accurately reflect the state of an organization's controls.

Key Questions:

- How granular is scoring / evaluation model to evaluate the control environment?
- What infrastructure exists to inherit assessment results from vendor-performed controls?

CONSISTENCY

When frameworks are vague, subjective, or free of maturity levels and scoring methodologies, it becomes difficult to gauge an organization's posture against that of another framework or even an industry baseline. This problem is compounded when assessment activities are not subject to quality and integrity reviews by an independent third-party assessor or certification body.

Key Questions:

- Can the effort result in a certification?
- How many entities issue these certification or opinions?

INTEGRITY

Simply put, the integrity of your assessment reports and assurances to internal and external stakeholders depends upon an audit and validation process during which trained external assessors evaluate your control requirements one by one and say things like: "Prove to me you're doing this," or "Show me where it's documented."

Key Questions:

- Is the Assessor's methodology, testing, and deliverables peer-reviewed by other firms?
- Are the assessor's methodology, testing, and deliverables reviewed by an accreditation and/or standards-enforcement body?



In addition to these criteria, it is important to consider **comprehensiveness** of the control framework, **prescriptiveness** and detail of the controls, **scalability** to any organization, and **efficiency** of assessments when determining reliability of results. All of these attributes will ensure a comprehensive approach to assurance.

Does every vendor need assurance?

As our HITRUST Risk Triage model indicates, a HITRUST assessment does not apply to vendors with negligible inherent risk, and vendors with very low or low risk are best suited to the e1 HITRUST assessment.

Assurance takes time and, for most vendors, it is a journey more than it is a destination. The HITRUST Vendor Risk Triage methodology is intended to align inherent risk with a minimum required level of assurance, not to replace the vendor's long-term cybersecurity, risk, and compliance strategy. Instead, vendors can prioritize demonstrating the required level of assurance in earnest, then enter into working relationships while more intensive forms of assurance are attained.

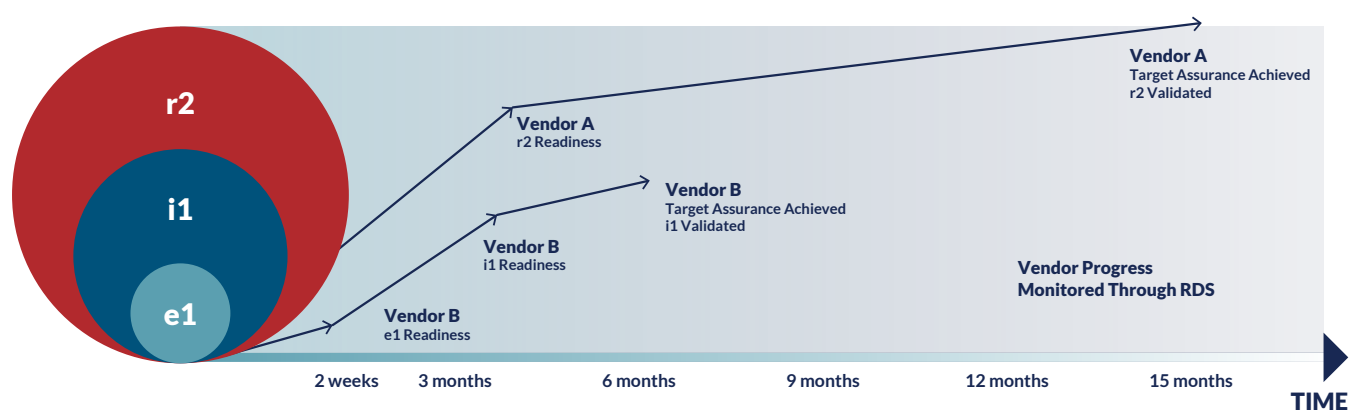
It is also important to note that a vendor's inherent risk is not fixed over time. For example, as Vendor ABC becomes more engrained in the organization and handles more data across more departments, its inherent risk will naturally increase and may result in an Inherent Risk Score of 5 that requires a higher level of assurance.





Using the HITRUST Risk Triage Model, organizations and their vendors can agree on a path to the targeted level of assurance in a reasonable time frame, with interim qualifying assurance achievements along the way. This prioritizes the working relationship of both parties while paving the way to stronger assurances across the entire industry.

The HITRUST Assurance Portfolio is reflective of this journey. Fully traversable, HITRUST provides a roadmap by which vendors can attain baseline assurances while building upon this foundational effort to attain higher level assurances over time. Through the Results Distribution System (RDS), organizations can monitor the progress of their vendors through successive, interim assurance achievements.



For more information, explore these other helpful resources.

**The HITRUST TPRM Methodology
Qualification Process Whitepaper**

**The HITRUST TPRM
Implementation Handbook**

**FOR MORE INFORMATION: Contact your HITRUST Product Specialist
Call: 855-448-7878 or Email: sales@hitrustalliance.net**

www.hitrustalliance.net