

# The Ultimate Solution to Managing Third-Party Cyber Risks



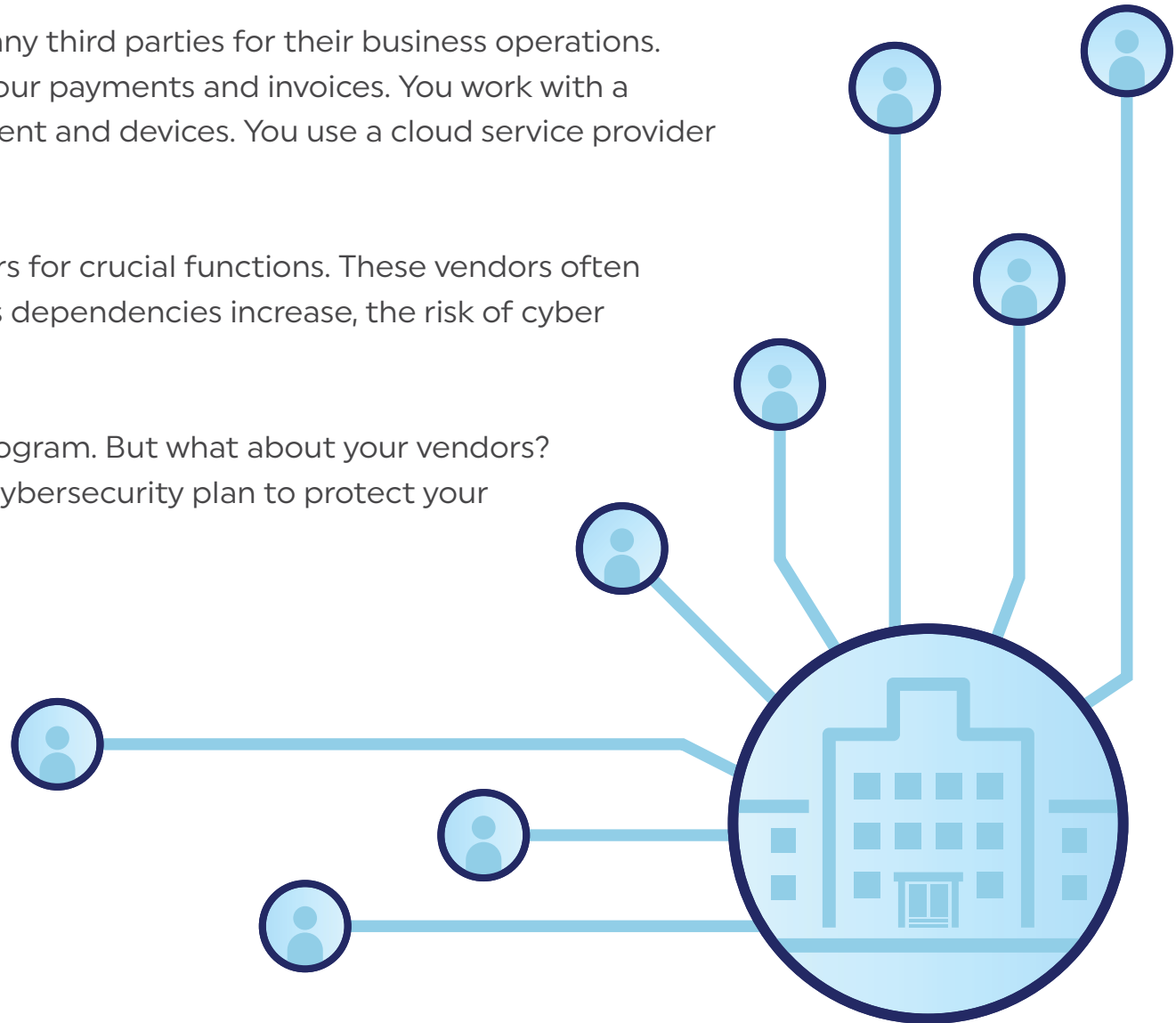
**HITRUST<sup>®</sup>**

## The Importance of Third-Party Risk Management (TPRM)

Companies, large or small, work with many third parties for their business operations. You may have a vendor who manages your payments and invoices. You work with a supplier that provides essential equipment and devices. You use a cloud service provider (CSP) to store your data on the cloud.

Organizations rely on third-party vendors for crucial functions. These vendors often gain internal access to sensitive data. As dependencies increase, the risk of cyber threats increases, too.

You may have a robust cybersecurity program. But what about your vendors? How do you ensure they have a strong cybersecurity plan to protect your and your customers' data?



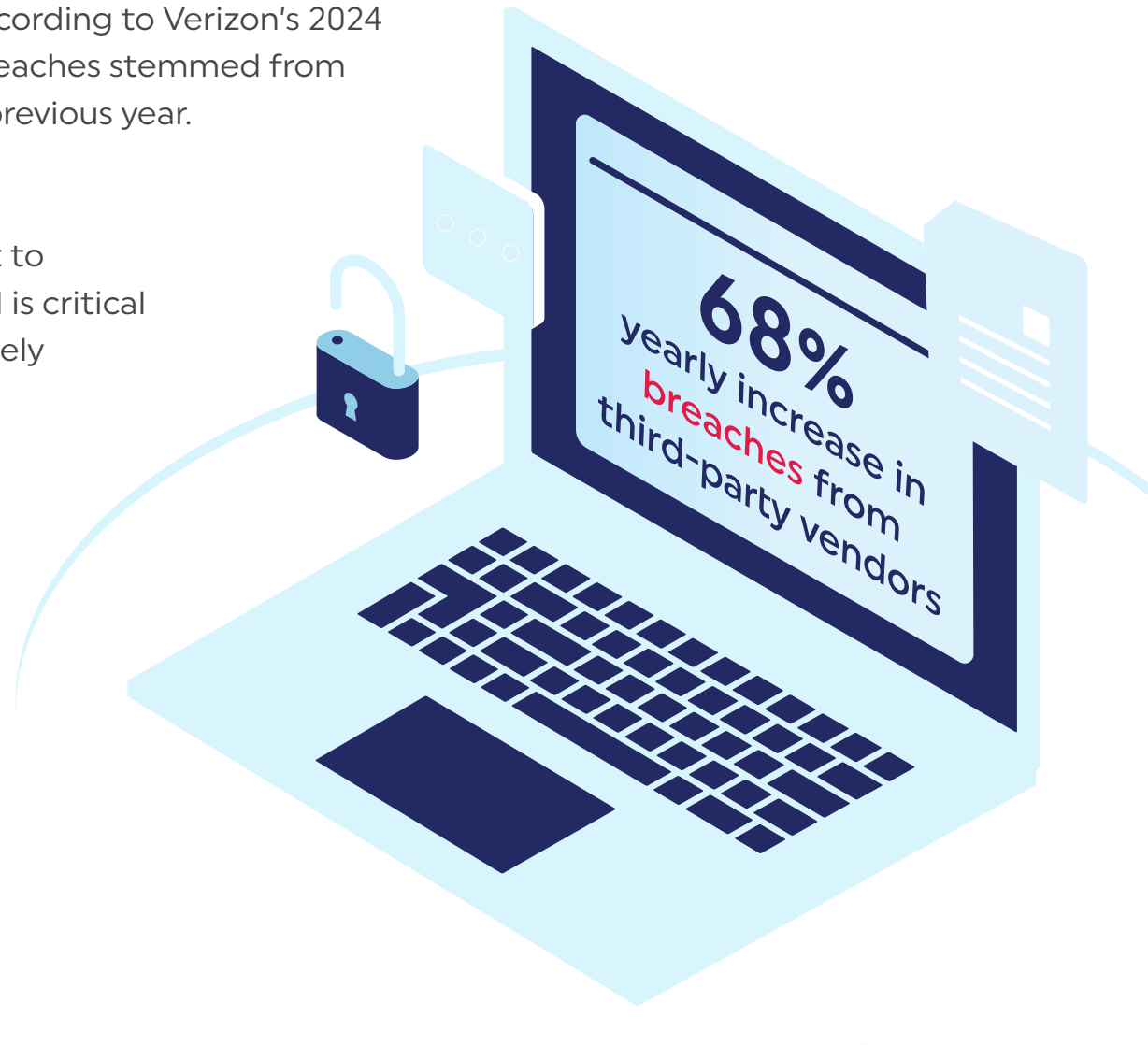
## Third-Party Risk Management is Broken

Organizations struggle to protect their data from attackers. Data breaches have become a common problem. According to Verizon's 2024 Data Breach Investigations Report, 15% of all breaches stemmed from third-party vendors — a 68% increase over the previous year.







Third-party partners are used as an access point to an organization's sensitive data. Effective TPRM is critical to ensuring your third-party vendors appropriately safeguard your data.

But all vendors are not the same. They differ in size, scope of work, risk profile, and cyber maturity. As you deal with varying volumes of diverse third parties, vendor risk management becomes challenging.



## Existing TPRM solutions are incomplete.

-  Most approaches to TPRM lack a consistent, standardized risk reporting approach.
-  TPRM teams have limited bandwidth and resources to follow through remediations.
-  TPRM teams can't keep up with the high volume of vendor assessments.
-  Vendors are overwhelmed with repetitive, proprietary questionnaires and audits.

To overcome these challenges, learn the best practices that will help you make cybersecurity TPRM effective.

# Best Practices to Enhance Cybersecurity TPRM

## Conduct standardized assessments

Ensure that your risk assessment is standardized and harmonized with global standards such as HIPAA, ISO, NIST, and GDPR. A standardized approach ensures consistency in evaluating vendor security postures.



The assessment should be based on relevant controls and frequently updated security framework. Make sure that the latest version of the framework incorporates latest threat data.



## Assess third parties based on their risk levels

Some vendors are at a higher risk than others. It is important to have a risk-tiering strategy to meet appropriate security requirements. Consistent risk analysis allows you to assess high-risk vendors without ignoring low-risk ones. When performing risk analysis, ask the following questions.

- **What data does the vendor process?**
- **If the vendor is attacked, how will it impact your organization?**
- **How important is that third-party vendor for your business?**
- **What are your responsibilities toward security and compliance?**

Based on your analysis, determine the correct level of security assurance needed for each third-party partner.

## Choose a reliable assurance mechanism

Choose a trusted, reliable assurance mechanism to ensure the third party takes proper security measures. Check if the assurance mechanism is known to reduce risk. The security framework should be well-recognized. Next, ensure that the assurance mechanism is consistent. The specified controls should be comparable to another organization's assurance report.

Go with an accurate assurance mechanism. It should use a detailed and quantitative scoring methodology. Finally, check if the assessment process is rigorous and thorough.

## Parameters of a reliable assurance mechanism





## Review CAPs to track progress

The assurance report suggests gaps in the security system. The next step for third parties is to create Corrective Action Plans (CAPs) to rectify control implementation. You must work with your third parties to ensure they take suitable measures to meet the gaps.

Check if the timelines are set correctly. Track progress continuously to improve efficiency in meeting the desired security outcomes.

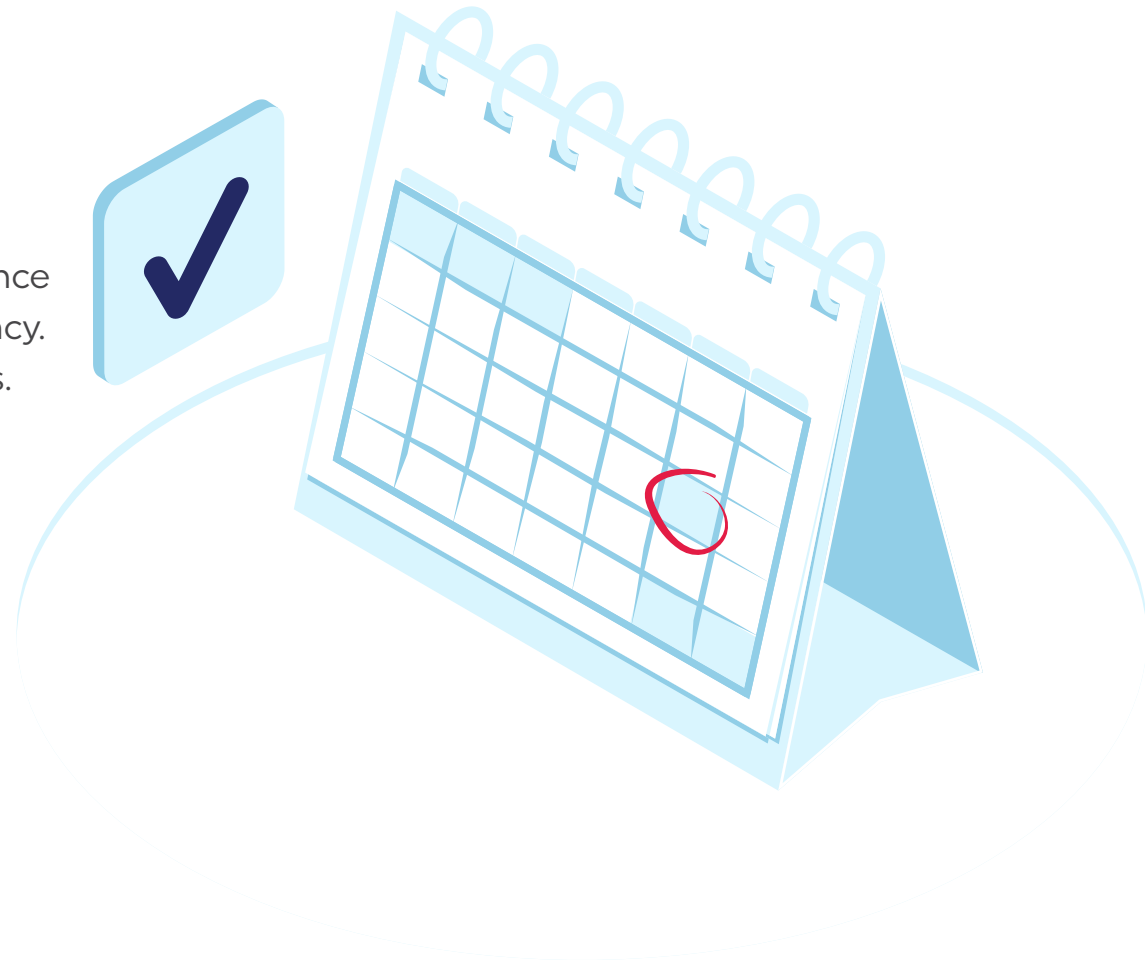


## Update assurance regularly

Security requirements are flexible and change constantly. New threats emerge with time. As the business grows, the potential risk level may increase, too. Sometimes, vendors may need to progress to a higher level of assurance.

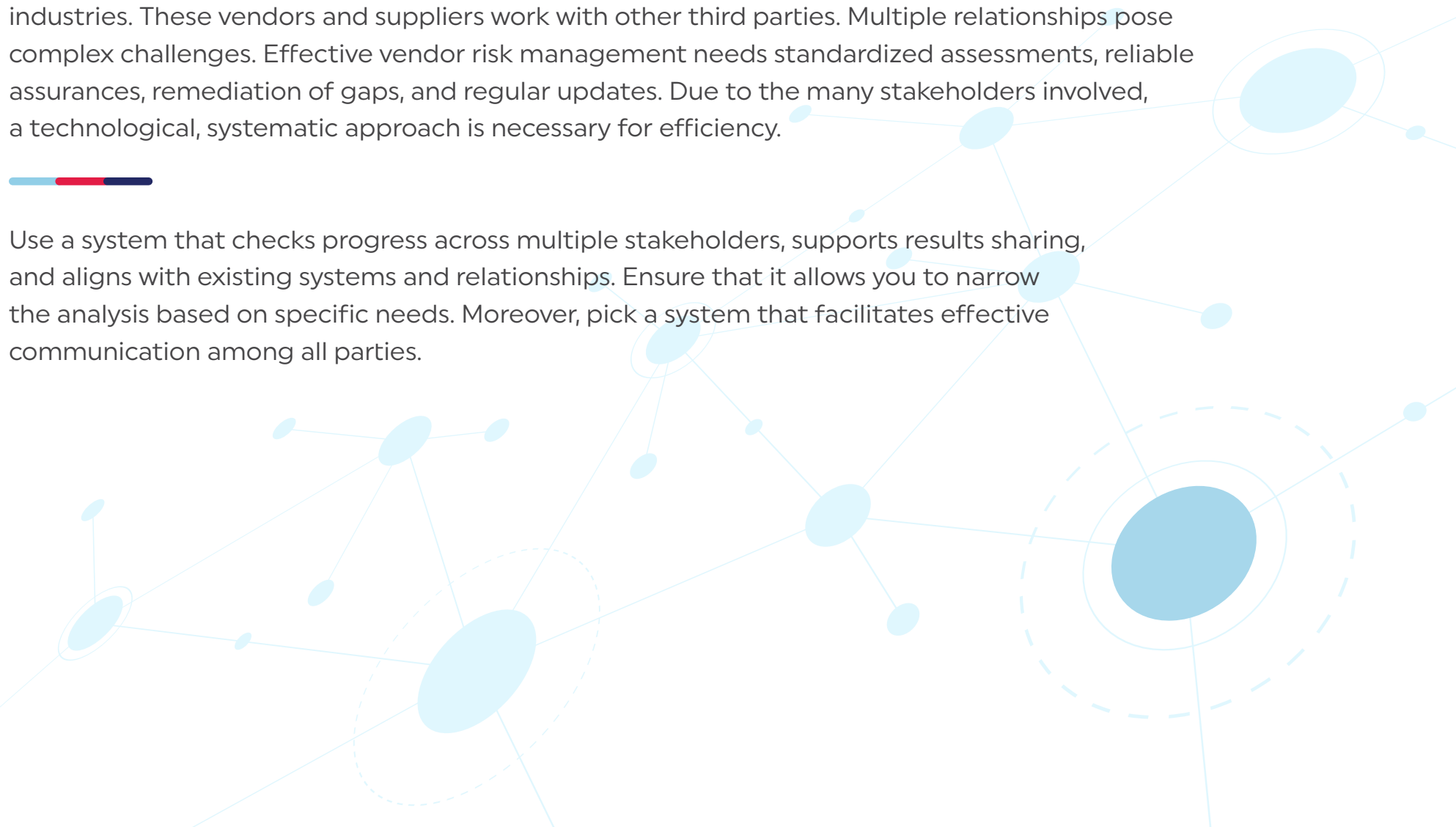
---

Assurance needs change based on several factors. This means third parties should update their assurance regularly. Updated assurance reports ensure relevancy. They prepare third parties against emerging threats.



## Use a systematic approach to manage multiple third parties

Your organization works with multiple third-party vendors and suppliers belonging to different industries. These vendors and suppliers work with other third parties. Multiple relationships pose complex challenges. Effective vendor risk management needs standardized assessments, reliable assurances, remediation of gaps, and regular updates. Due to the many stakeholders involved, a technological, systematic approach is necessary for efficiency.



Use a system that checks progress across multiple stakeholders, supports results sharing, and aligns with existing systems and relationships. Ensure that it allows you to narrow the analysis based on specific needs. Moreover, pick a system that facilitates effective communication among all parties.

## HITRUST Helps in Effective Cybersecurity TPRM

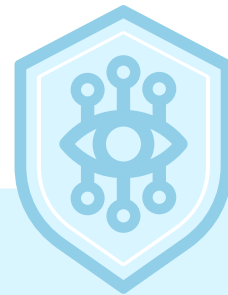
The simplest way to implement these best practices is by choosing HITRUST.



HITRUST is the only assurance mechanism proven to reduce risk.



The HITRUST framework harmonizes over 60 global standards.



HITRUST stays ahead of emerging threats with threat intelligence data.



HITRUST offers scalable assessment options based on vendor's risk profile.



HITRUST reduces manual effort and streamlines vendor management.



HITRUST encourages continuous risk tracking and remediation.

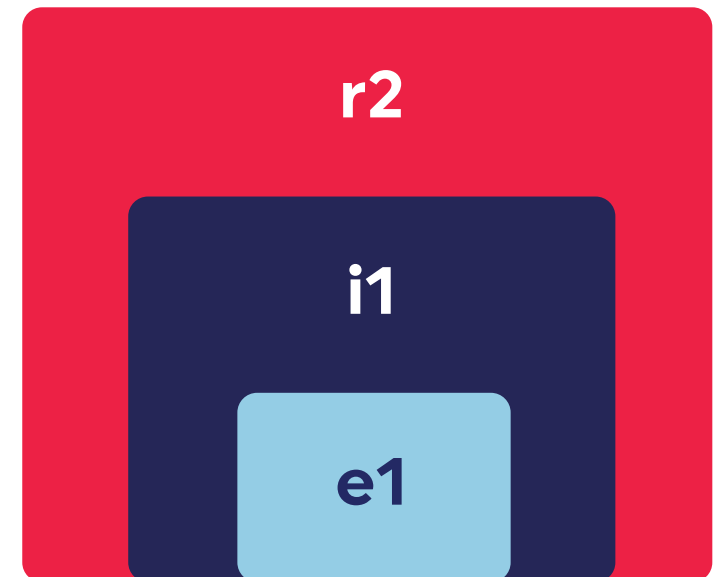
## HITRUST Assessment Options

HITRUST offers three core security assessment options based on vendor needs, size, risk maturity, and business profile.

- **The HITRUST e1 Assessment** is ideal for low-risk vendors seeking to establish critical cybersecurity controls or more complex organizations looking to start their certification journey with plans to move into a more comprehensive assurance level.
- **The HITRUST i1 Assessment** offers more coverage than the e1. It is suited for third-party vendors demonstrating leading security practices.
- **The HITRUST r2 Assessment** is the most comprehensive assurance. It is considered the gold standard in the industry and is ideal for high-risk vendors.

Each level is built on a common framework. This means your third-party partner can begin with a lower-level assessment and move up to a higher level without losing the invested time, money, and effort.

### Assessment levels

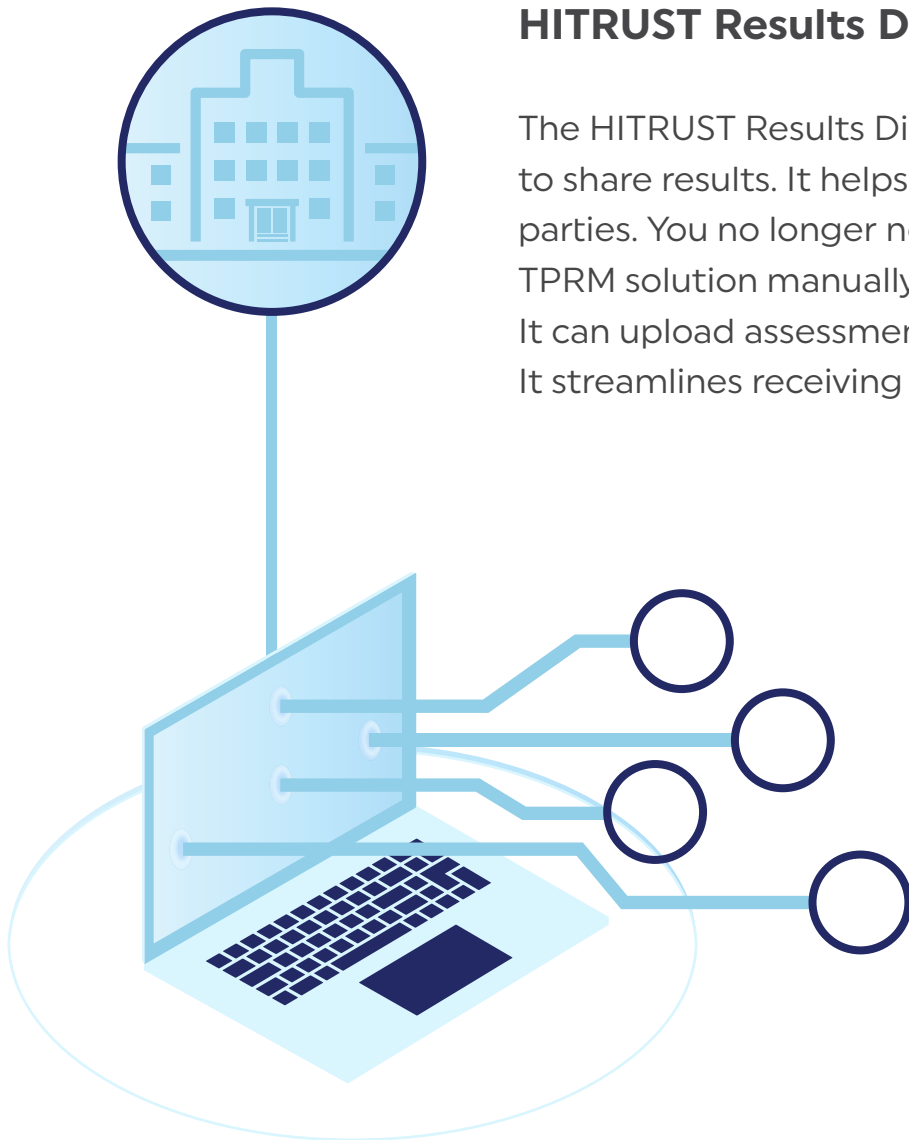


## HITRUST Results Distribution System (RDS)

The HITRUST Results Distribution System (RDS) offers a secure electronic portal to share results. It helps you save time and effort when managing multiple third parties. You no longer need to locate assessment results and enter data into your TPRM solution manually. The RDS enables better compliance and analytics. It can upload assessment details into TPRM solutions instantly and efficiently. It streamlines receiving and analyzing assessment results.

## HITRUST Assessment XChange

The HITRUST Assessment XChange streamlines vendor evaluation and compliance tracking by automating manual processes and reducing administrative burdens. With customizable vendor follow-ups and a managed service approach, organizations can enhance responsiveness while focusing on strategic initiatives. Through integration with platforms like ServiceNow, the HITRUST Assessment XChange enables organizations to seamlessly request, track, and analyze HITRUST assessment data within their existing workflows, ensuring a more efficient and scalable vendor risk management process.





With its suite of products and services, HITRUST offers the most comprehensive assurance mechanism. It makes the third-party assessment process effective. It facilitates seamless communication among all stakeholders and helps them meet common expectations. For the ultimate solution, choose HITRUST and enhance cybersecurity TPRM for your organization.

Learn more about managing third-party cyber risks here:  
<https://hitrustalliance.net/third-party-risk-management>