

The Ultimate Solution to Managing Third-Party Cyber Risks



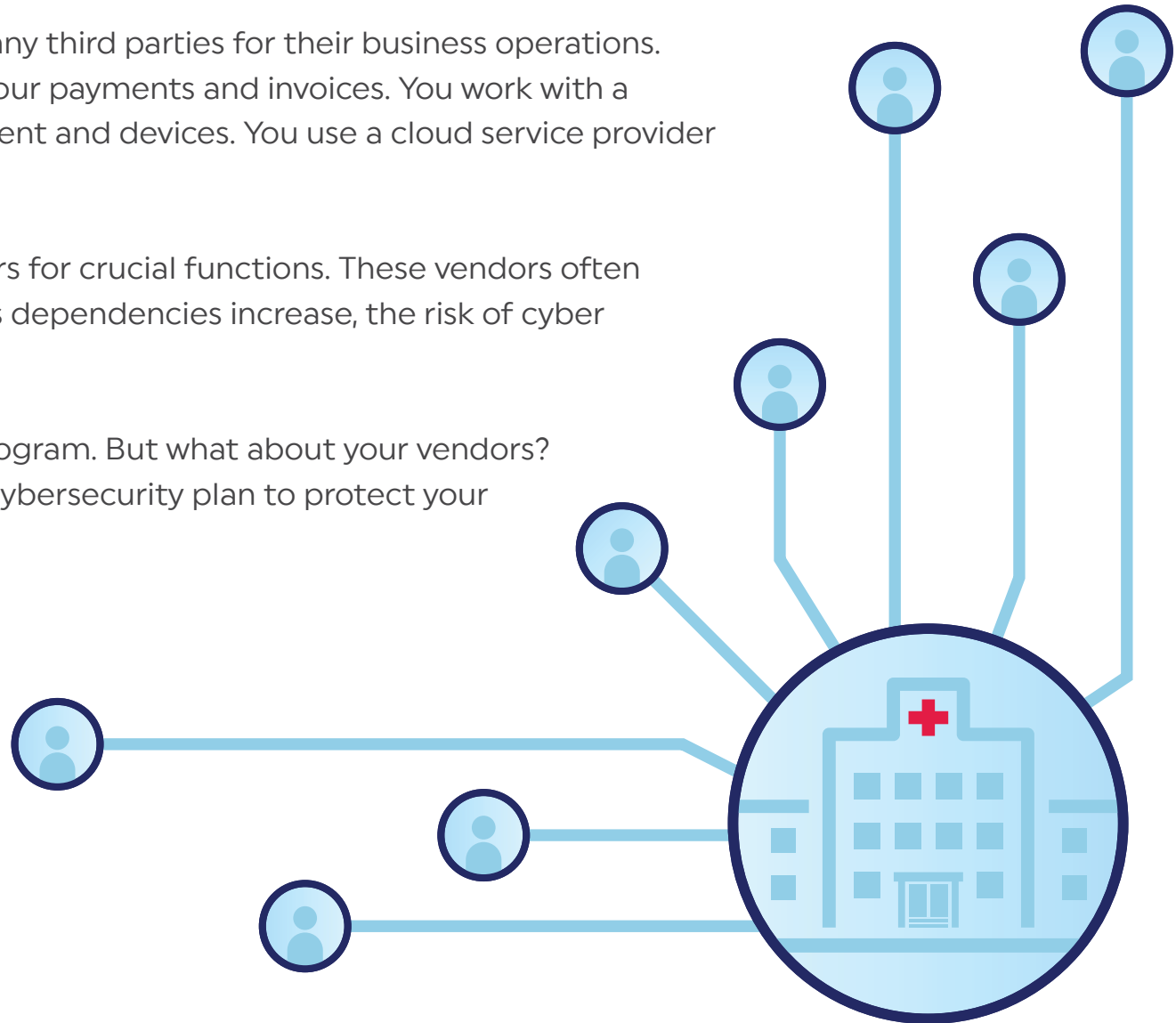
HITRUST[®]

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?



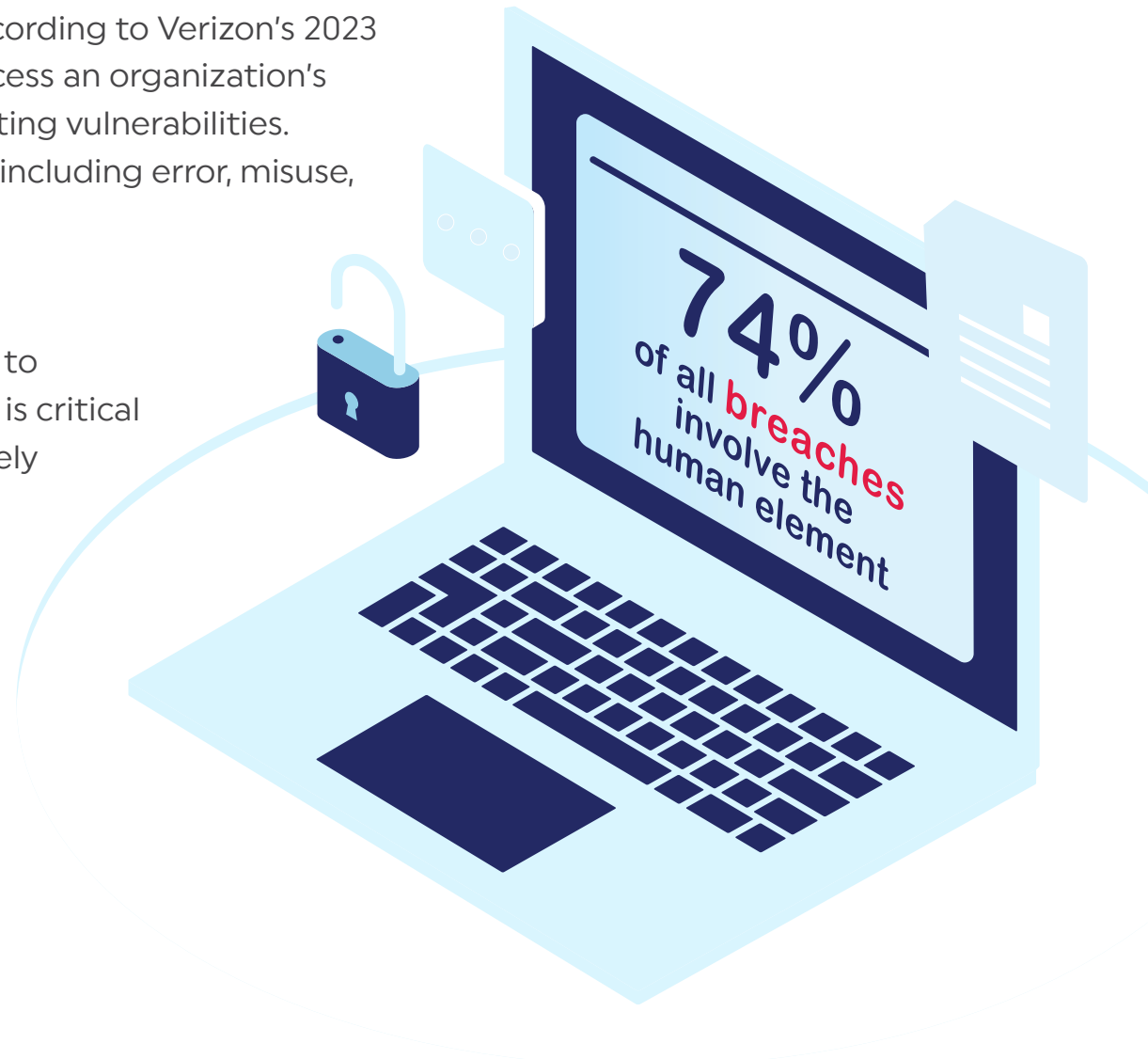
Third-Party Risk Management is Broken

Organizations struggle to protect their data from attackers. Data breaches have become a common problem. According to Verizon's 2023 Data Breach Investigations Report, attackers access an organization's data by stealing passwords, phishing, and exploiting vulnerabilities. 74% of all breaches involve the human element, including error, misuse, and social engineering.







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, widely available risk reporting approach.
-  TPRM teams have limited bandwidth and resources.
-  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 TPRM efficient.

Best Practices to Enhance TPRM

Use clear language in contracts

Ensure your contract language is clear and concise. All stakeholders should have a common understanding of the contract. Define the expectations of all parties. Choose a standard mechanism to determine what is being protected. Clarify acceptable measures in assessing security maturity.



The contract should specify the scope of the system and data. It should support risk assessment and ensure all stakeholders have common assurance expectations. Further, the contract should mention data ownership, use, and management requirements, along with risk management and security expectations.



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

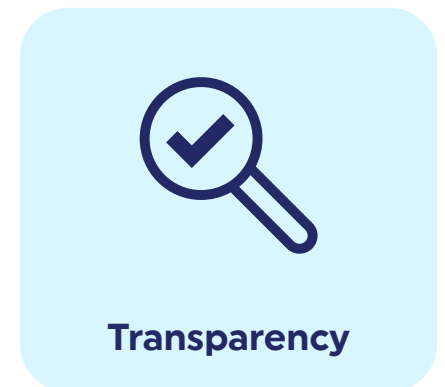
Based on your analysis, determine the correct level of security assurance needed for each third-party partner.

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 transparent. You should know the source of the controls. The control system should be well-recognized. Next, ensure that the assurance mechanism is consistent. Assessment results should be the same irrespective of the assessor. 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 that the assurance mechanism maintains integrity. Ensure the assessors are trained and conducting assessments faithfully.

Parameters of a reliable assurance mechanism





Review CAPs to track progress

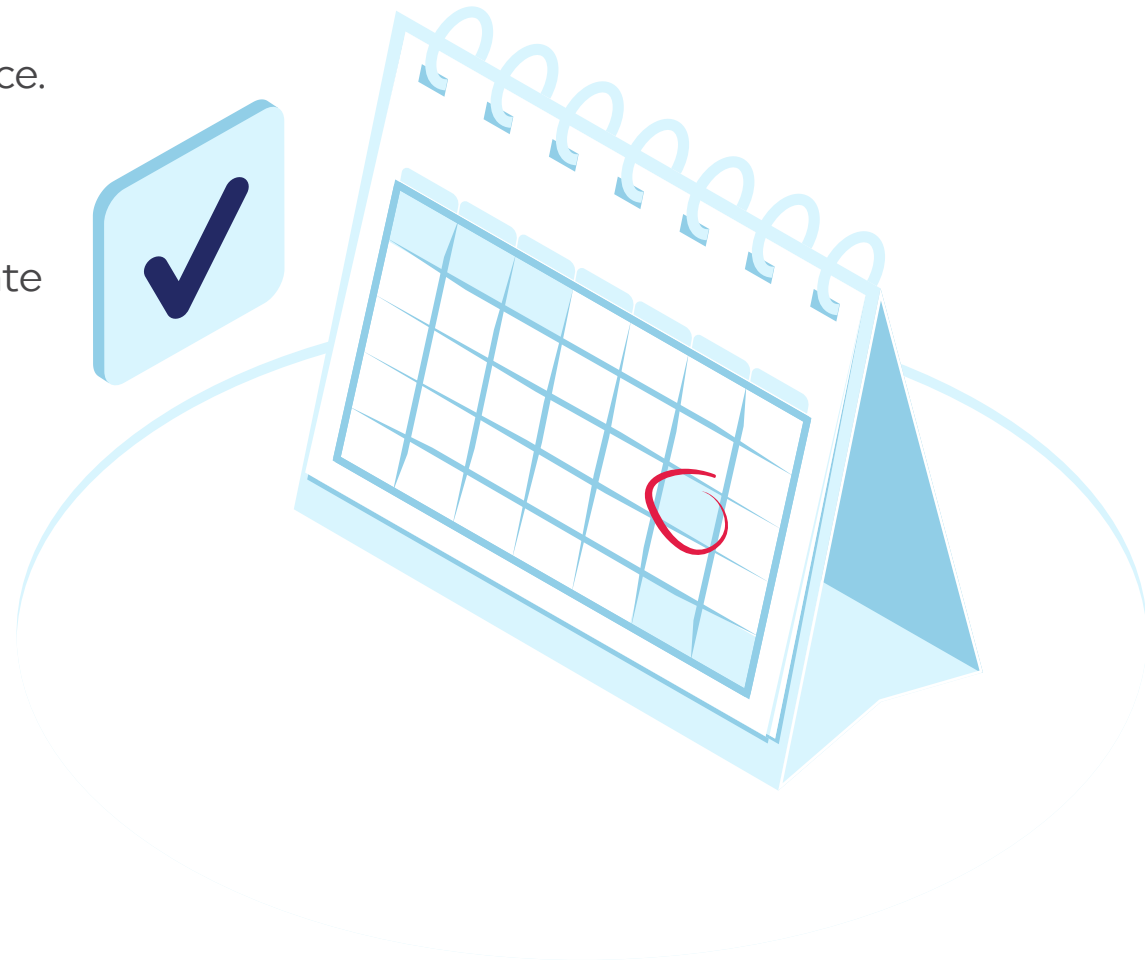
The assurance report suggests gaps in the security system. The next step for third parties is to create Corrective Action Plans (CAPs) to rectify control implementation. You must work with your third parties to ensure they take suitable measures to meet the gaps.

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 clear expectations, documented 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 Efficient TPRM

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



HITRUST offers reliable assurances that are based on the HITRUST CSF.



The CSF is accepted widely.



You can access the CSF easily to determine the sources of the controls.



The CSF is mapped to multiple authoritative sources, ensuring consistency.



The HITRUST scoring methodology is based on a quantitative model, making the results unbiased and accurate.



HITRUST trains assessors to follow a standard process, ensuring integrity.

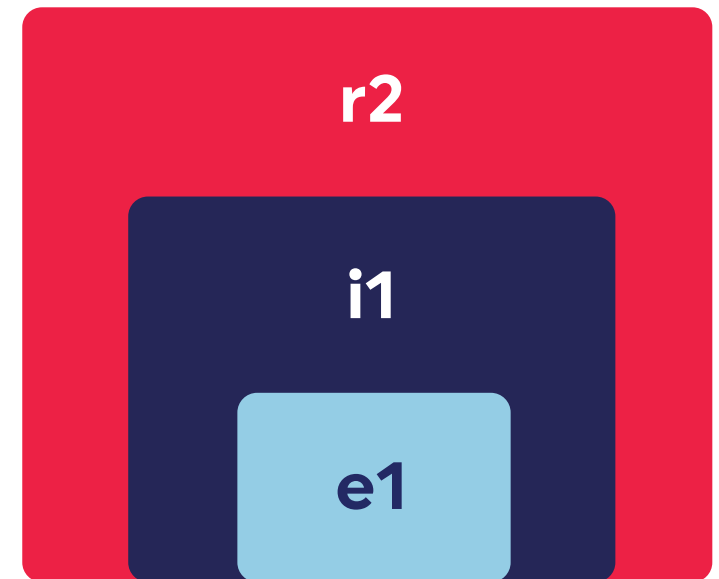
HITRUST Certification Options

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

- **The HITRUST Essentials (e1) Validated Assessment** is ideal for low-risk vendors seeking to establish basic foundational cybersecurity or more complex organizations looking to start their certification journey with plans to move into a more comprehensive certification level.
- **The HITRUST Implemented (i1) Validated Assessment** offers more coverage than the e1. It is suited for third-party vendors demonstrating leading security practices.
- **The HITRUST Risk-Based (r2) Validated Assessment** is its 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.



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

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