Vanta

Vendor Risk Assessment Checklist:

A Rubric to Get You Started

Low	Low	Low	Medium	High
Low	Low	Medium	Medium	High
Low	Medium	Medium	High	High
Medium	Medium	High	High	Extreme
Medium	Medium	High	Extreme	Extreme

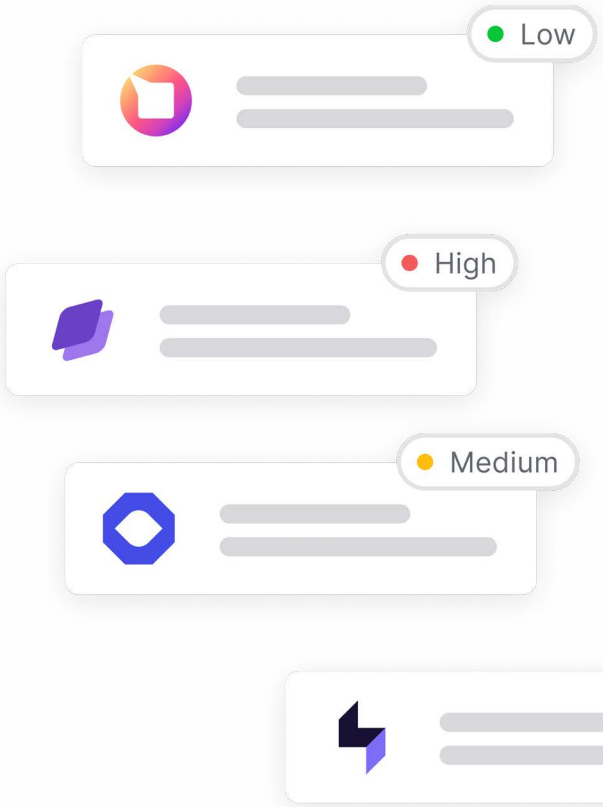
Introduction

Third-party risk management (TPRM) is a crucial practice for today's businesses. Any third-party tools, software vendors, contractors, and even browser plug-ins that are connected to your systems and operations could introduce new risks to your environment.

For example, a software tool integrated with your systems could become a pathway to your critical data if breached. Or if a core vendor experiences an outage or makes a logistical error, it could halt your entire organization. These types of scenarios can lead to financial fallout, customer churn, and reputational risk.

Conducting security reviews assessing the potential risk of utilizing a vendor's product or service—is a key step in identifying and mitigating these types of risks. Because a vendor's environment can (and will) change, teams must conduct these reviews regularly as part of their TPRM initiatives.

The average organization uses hundreds or even thousands of vendors—this many vendors can be challenging to manage. This often results in inconsistent and ineffective vendor security reviews. Organizations must prioritize monitoring and reviewing vendors that present the most **inherent risk.** Conducting objective risk assessments ensures that resources are spent wisely and eliminates guesswork or assumptions that can come with security reviews.



Checklist: How to conduct inherent risk assessments

A successful third-party risk assessment process helps establish a stronger security program. A risk assessment rubric is the foundation for the rest of your risk management activities, such as conducting regular security reviews, maintaining compliance, and building and enforcing effective policies.

After completing the steps in this checklist you'll be able to map your risks within a rubric, like the one pictured below. This rubric will help you visualize all the potential risks your organization faces and prioritize them against the likelihood of each risk scenario and their potential impact.

Here's how to conduct an inherent risk assessment for your organization:

- [ ] **Step 1: Understand your company's risk management goals.**
- [ ] **Step 2: Create a rubric for defining inherent risk.**
- [ ] **Step 3: Collect data to fill in the rubric.**
- [ ] **Step 4: Calculate the inherent risk score.**

Inherent risk vs. residual risk

When we talk about inherent risk, we mean the level of risk a particular vendor would pose to your organization if something went wrong. Inherent risk is based on factors such as the vendor's role and level of access to your data and systems.

Residual risk, on the other hand, refers to the level of risk that remains after security controls and other mitigations have been implemented.

LIKELIHOOD \ IMPACT	Insignificant	Minor	Moderate	Major	Critical
Rare	Low	Low	Low	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Possible	Low	Medium	Medium	High	High
Likely	Medium	Medium	High	High	Extreme
Almost certain	Medium	Medium	High	Extreme	Extreme

- **Low:** Accept the risk, routine management
- **Medium:** Specific responsibility and treatment
- **High:** Quarterly senior management review
- **Extreme:** Monthly senior management review

Step 1: Understand your company's risk management goals.

Every organization has a different way of thinking about and calculating risk. Risk appetite—the amount of risk that an organization is willing to accept to achieve its objectives—will vary based on your industry, company size, and other factors. For example, a customer service-oriented business would likely prioritize risks to service interruptions, while a financial services organization would prioritize risks that could lead to fraud or non-compliance.

To understand your organization's risk management priorities, start by interviewing stakeholders, such as the leadership team. These conversations can give you a deeper understanding of which data is essential to the business and where that data lives. This will help you understand the business's risk appetite. As opinions about risk management will vary within your organization, achieving consensus and balancing business velocity with security are important.

Step 2: Create a rubric for defining inherent risk.

Next, your team needs to know which quantitative data to collect to define inherent risk. Laying out a rubric based on your unique business needs and risk factors can help you anticipate the information you need to collect from the right parties.

Here's a recommended rubric format to get you started:

TYPES OF DATA PROCESSED
Does the vendor process or have access to any sensitive, private, or otherwise risky data? Some common types of sensitive data include: → Customer data—directly or indirectly provided by the customer (e.g., PII or customer metadata) → Cardholder data → Intellectual property and trade secrets → Employee data → Financial or cardholder data → Personal health information (PHI) → Metadata, such as corporate email addresses, employee handbooks, or other corporate policies

BUSINESS CRITICALITY

Rank the level of business criticality using the following categories:

- → **Minor effects:** Downtime would minimally affect operations or not impact them at all. (Example: A marketing tool that isn't critical to your organization's daily operations.)
- → **Major effects:** Operations would be degraded. (Example: Customer support platform.)
- → **Critical effects:** Operations would be halted entirely. (Examples: Cloud storage providers or finance/payments platforms.)

INTEGRATION ACCESS

What permissions and access does the vendor have to your systems? Integration access can fall into one of the following categories:

- → **Read internal systems:** The vendor can view or read data from internal systems (e.g., marketing or recruiting tools).
- → **Read production systems:** The vendor can view or read data from the production environment (e.g., data analytics or engineering tools).
- → **Write or modify internal systems:** The vendor can modify or write data to internal systems (e.g., document management or identity provider tools).
- → **Write or modify production systems:** The vendor can modify or write data to production systems (e.g., cloud providers or data storage/processing tools).

COMMUNICATION ACCESS

Vendors that can communicate on your company's behalf to key groups like employees, customers, or shareholders carry more inherent risk, as negative repercussions could occur if unauthorized parties gain access to their systems.

Step 3: Collect data to fill in the rubric.

Next, collect resources from internal and external stakeholders to provide insights for the above rubric. A few good places to look include:

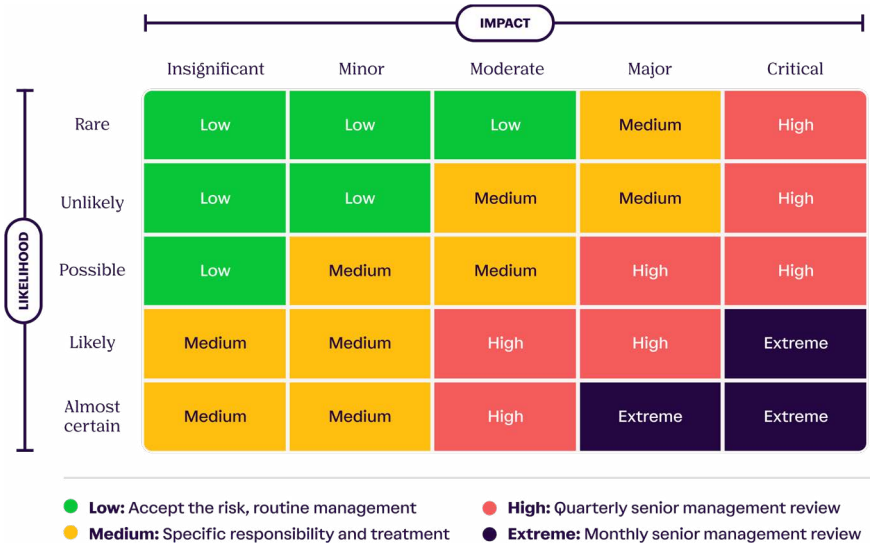
- Internal resources about vendor relationships, such as scopes of work, SLAs, contracts, etc.
- Security questionnaires for cybersecurity risks.
- Vendor interviews for operational and strategic risks.
- Due diligence for financial, compliance, and reputational risks.

Track all findings in a centralized document or your vendor risk management platform.

Step 4: Calculate the inherent risk score.

Finally, use the data collected to calculate the likelihood of occurrence and magnitude of impact on your organization. The individual rankings within your inherent risk assessment should roll up into scores for likelihood and impact. Then, you can calculate the final risk score with the formula: **Risk Score = Likelihood x Impact.** Once you have this score, you can plot all of your risks within your risk rubric to visualize your organization's risk.

You'll then use these calculations to prioritize your vendor reviews. This strategic prioritization ensures that you work toward managing and mitigating the most high-risk vendors within your organization first and foremost.



Unmanaged vendors and inherent risk

As you conduct inherent risk assessments on your existing vendors, consider the possibility of unmanaged vendors or applications. Even when teams have policies in place to prevent shadow IT, almost all businesses have at least a few unsanctioned apps hanging around.

Many businesses use VRM automation software to detect new vendors connecting to their infrastructure. Vanta helps customers uncover unmanaged external resources by automatically listing all third-party applications.

Introducing Vanta

With Vanta, you can create a color-coded risk assessment matrix with a few clicks. By default, the platform helps score risks for likelihood and impact on a scale of 1–5. You can even use custom categories and scoring options to build a tailored risk matrix.

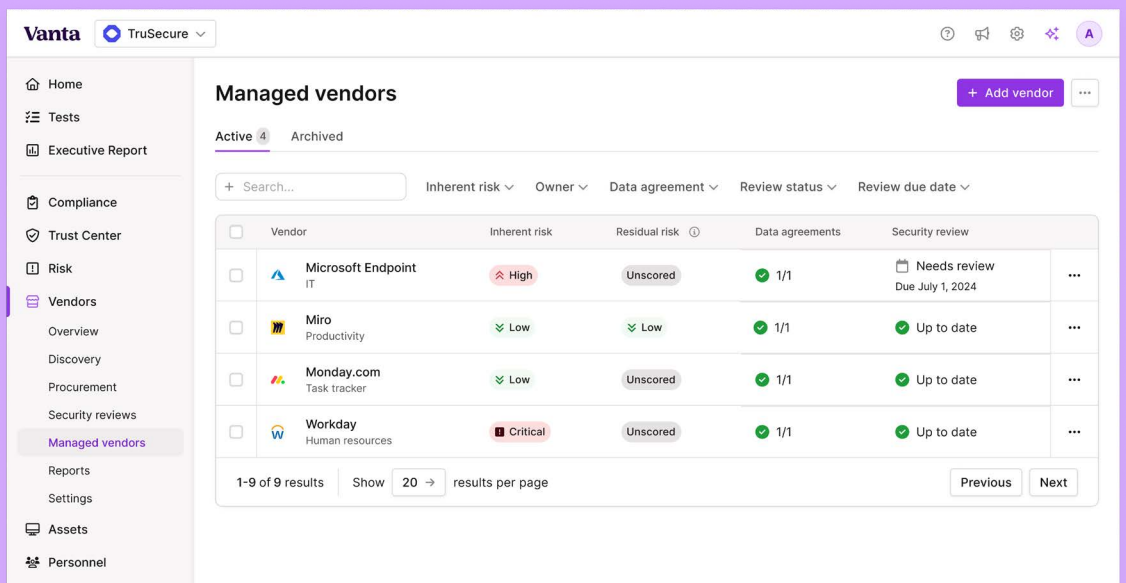
We automate all stages of managing third-party risk, including:

- **Assigning risk scores** to vendors based on the inherent risk rubric and any customization that you want to add based on your unique business.
- **Streamlining the process** of sourcing and parsing vendor security information.
- **Identifying risk trends** over time and setting up re-assessment cadences based on inherent and residual risks.
- **Discovering all vendors** within your ecosystem, centralizing vendor inventory, and kicking off risk assessments from a single platform.

> "Vanta's Vendor Risk Management solution slashed the time I spend on ongoing vendor security assessments from one full day to only one hour each week. As a result, we've absorbed double the volume of questionnaires without adding headcount."
>
> **Vicky Levay, Sr. Director, Compliance, Risk, & Information Security**
> FloQast

Ready to simplify and streamline your third-party risk management program?

Request a demo today ›



Vanta

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. Thousands of companies, including Atlassian, Chili Piper, Flo Health and Quora, rely on Vanta to build, maintain and demonstrate their trust—all in a way that's real-time and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, New York, San Francisco and Sydney.

Request a demo →

VANTA.COM