

Serious security professionals use people-first third party risk management.



THE HOW-TO GUIDE  
FOR SERIOUS SECURITY PROS:

# Building A Third Party Risk Management Program



**OSTENDIO**



# Introduction

## Your Complete Guide To Third Party Risk Management

According to the 2021 Ponemon Institute Report, 74% of companies that experienced a data breach reported that the root cause of the breach originated from a third-party. While you can never truly eliminate third party risk, you can certainly manage it.

Not only does a third party risk management (TPRM) program work to mitigate vendor risk, serious security people who have a robust system of practices and procedures in place gives their organization the ability to move swiftly and effectively when onboarding, and offboarding a third party.

This eBook provides the appropriate building blocks needed to establish an effective people-first TPRM program that leverages the power of your greatest asset... your people.

### We'll Cover

1. The State Of Third Party Risk
2. Third Party Risk Management Mistakes To Avoid
3. Third Party Risk Challenges & How To Solve Them
4. 3 Steps To Building An Effective Program



# The State of Third Party Risk

## What Is Third Party Management?

Third party risk management is the process of identifying and managing risk associated with the use of third parties. This is an organized system that involves analyzing, controlling, tracking and mitigating the risks that come with outsourcing vendors, contractors, suppliers, and service providers. Third party risk comes in many forms: strategic, reputation, operational, transactional, compliance and information risk.

## Third Party Risk Management Vs. Vendor Risk Management?

The term “third party” encompasses all third parties that your organization employs and interacts with, such as cloud-based hosting providers, SaaS software solutions, and agencies. “Vendor” describes a specific type of third party, such as a service provider, manufacturer, or wholesaler of goods to your organization. Each third party, whether a vendor, supplier, or other third party comes with its own unique set of risks that need to be analyzed, identified and monitored.

## Why Do I Need A Third Party Risk Management Program?

Most organizations today work with a third party of some kind. According to Gartner’s Third Party Risk Management Report, 71% of organizations say their third party network has grown in the last three years, making risk management a top priority. Chances are, your third party network is growing too—whether you’re onboarding contractors, outsourcing department operations, or integrating third party systems. And don’t be fooled by the “big players.” They can be just as vulnerable

## Growing Need For Third-Party Risk Management:

**87%**

of firms have experienced a third party incident that disrupted operations

Source: Deloitte Global Survey on Third Party Governance and Risk Management

**51%**

of businesses report they’ve suffered a data breach caused by a third party

Source: Ponemon Institute

**83%**

of executives report that third party risks were identified after initial onboarding.

Source: Gartner



The problem?  
Organizations are not devoting the appropriate resources to managing third party risk.

to cyber threats as any company—if not more with millions of data points enticing cyber criminals to attack.

When you don't have enough eyes on third party risk, you create a domino effect: not enough staff dedicated to TPRM leads to overworked employees, which leads to human error which can lead to granting too much privilege to third parties or overlooking high-risk vendors.

A TPRM program is your first line of defense against cyberthreats that originate from outside your organization. And in this day and age, the move to cloud-based services reinforces the need for third party risk measures. You should ask yourself: are these third parties you interact with handling your data appropriately? What information should they (or should they not) have access to?

An effective program will give your organization the necessary steps to analyze third party risk, take additional steps if needed, and appropriately audit and monitor vendors continuously.

# Avoid These Third Party Risk Management Mistakes

## 1. **Failing To Recognize The Significant Risk Vendors Pose To Your Organization**

Having a security program for your own business, doesn't guarantee that your vendors have an equally secure system in place. Don't make the mistake of assuming vendors are secure or thinking that is their issue to deal with. The end result could impact the value of your brand, stock and future business.

## 2. **Assuming That Large Or Established Vendors Have A Strong Security Program In Place**

No organization is immune to security breaches, big or small. Don't make the mistake of assuming that a large vendor must have a strong security program or is secure because you have worked with them for an extended period of time. For example, when an established business like Zendesk suffered a security breach by an unauthorized third party, it ultimately affected 10,000 accounts which also included the FCC and Uber.

**The bottom line: large organizations that you might reasonably assume to have a robust security program in place can also experience security breaches.**



## What To Look For

### In An Integrated Risk Management Platform

Look for a platform that is easy to navigate, is integrated into your overall security program and keeps all your records up to date. Consider the standards and regulations that your business follows and make sure that the system you choose is constantly keeping up to date with the standards as they change to ensure your third parties remain compliant.



## Avoid These Third Party Risk Management Mistakes

### 3. **Not Running A Third Party Risk Assessment On An Annual Basis**


Some organizations feel that a one-time third-party risk assessment is sufficient. Cyber criminals are relentless and are constantly changing and adapting their tactics to gain access to protected or sensitive information. Your business needs to be constantly working to be one step ahead of the hackers. Keeping vendor risk assessments up-to-date annually alerts you to their vulnerabilities.

### 4. **Failing To Include All Your Vendors In A Vendor Risk Management Program**

Many companies make the mistake of using vendor risk management for only a restricted number of vendors that exceed certain thresholds of contract value or other metrics, but any third party with ANY amount of access to your systems or data poses a risk that must be documented and monitored. If you know that one of your vendors has experienced a breach, make sure they document how it was handled and demonstrate the steps they've taken to prevent reoccurrence.

### 5. **Not allocating a budget to protect your business.**

The average data breach cost \$4.24 mill. & businesses who aren't compliant may also suffer financial penalties or even loss of business.



# Third Party Risk Management Challenges (And How To Tackle Them)

Establishing third party risk management comes with challenges. We've compiled a quick list of the most common third party risk management hurdles and how you can address them as you work through building your program.

## CHALLENGE #1

- **Using outside staff & experts for assessments is costly & time-consuming.**

Some companies choose to use experts to complete questionnaires, which can be time-consuming & expensive since they have to manually map inbound assessments with data already held by the organization. This can be laborious when external consultants are unlikely to be familiar with an organization's internal controls.

- **What you can do:**

Find an integrated risk management software that allows you to store documentation & evidence that shows your company's policies in order to pass security audits & meet requirements of various standards & frameworks. When a third party assessment is requested, you can then easily map the evidence to the relevant questions.

## CHALLENGE #2

- **Centralized vendor assessment repositories require more effort.**

A centralized vendor assessment repository allows a company to store all of their vendor responses & allow customers to source this information, but these questionnaires require information in different formats & it's not an easily repeatable process. This repository is often offline & the information quickly becomes out of date, requiring a level of effort to manually maintain—thus creating more of a problem than the repository is solving.



## How to tackle challenges

- **What you can do:**

Look for a solution that allows you to store up-to-date data in real-time. This means there is no need for any centralized vendor assessment repository because the platform holds the latest information & is complete with version control & approvals. The ideal solution should make it simple to respond to customized assessments by mapping information already maintained on the platform to the customer questionnaire. map the evidence to the relevant questions.

### CHALLENGE #3

- **Shared assessments are manual & labor-intensive.**

Fundamentally, a shared assessment provides a detailed report about a service provider's controls & standardizes many of the controls & alignment with a system like NIST CSF. & while using shared assessments has become more popular, ultimately, this is still a "spreadsheet" process & not everyone in an organization uses it. There is still a desire for customization & to add proprietary questions.

- **What you can do:**

Opt for a fully integrated risk management platform that includes all employees in building a culture of security in an organization. This kind of system does away with manual forms & questionnaires & makes spreadsheets a thing of the past.





# How To Build Your Third Party Risk Management Program

## **Step 1:** Track The Number Of Organizational Vendors & Third-Parties

As organizations continue to increase the number of vendors they work with, tracking individual security capabilities has become exponentially more challenging. In the past, organizations could focus on protecting the data that they manage directly, and even when they did work with a third party, the third party's product was often implemented within their own network environment. Today, everything from our production hosting environment to sales and marketing tools, financial accounts, and even the way we communicate is often provided by a cloud-based third party.

This makes it even more challenging to know where data might be, let alone ensure that your vendor is protecting it appropriately. Even renowned, everyday technology companies have demonstrated a clear disregard for implementing effective security protocols. For example, Zoom recently was forced to pay an \$85M fine after the FTC alleged that they "engaged in a series of deceptive and unfair practices that undermined the security of its users."

## **Step 2:** Assess Vendors By Risk Level

Developing an effective third party risk management program ensures companies are protecting data they manage directly and have a mechanism to understand the level of risk involved when they share data outside of their organization.

While not all vendors will have access to sensitive data, and therefore the risk may not be as consequential, it is critical for companies to assess vendors by risk level and set relevant mechanisms in place to ensure that those who do have access to data are taking the appropriate measures to protect it.



## **Step 3:** **Select An Integrated Risk Management Tool To Assess Vendor Risk**

### **How do you start a vendor risk management program?**

As Gartner outlined in their recent report Emerging Technologies: Top Use Cases in Integrated Risk Management, client companies should not approach a vendor risk management program as an independent process, but as part of a fully integrated risk management program. As mentioned in Step 2, Ostendio recommends that companies start by assessing all of their vendors by risk category and reserve the most scrutiny for those categorized as highly critical and critical.

A select number of integrated risk management platforms, such as the Ostendio platform, allow customers to sort vendors by risk category and for customizable assessments to be sent directly to all vendors with the content of the assessment tailored to the criticality of the risk. This process ties the vendor's response directly to the organization's own security and risk management program and enables the organization's vendor to use their own free version of Ostendio to simplify and organize their response.

Once a Ostendio Trust Network connection has been established between an organization and its vendor, an assessment can be scheduled to run on a routine basis, for example yearly. This allows companies to regularly check on the risk category of all their vendors.



## About Ostendio

Ostendio's Ostendio™ helps companies to build, manage and demonstrate their information security framework. The Ostendio platform provides an enterprise view of an organization's cybersecurity program. Ostendio's unique bottom-up security approach provides a workflow solution which engages every employee and manages all aspects of security and compliance which allows organizations to easily report their security posture to internal and external stake-holders. With Ostendio, customers can ensure they are secure and compliant.

Ostendio is headquartered in Arlington, VA and has customers in North America, Europe, the Middle East and Australia. For more information about Ostendio's Ostendio, please visit [www.ostendio.com](http://www.ostendio.com).

## Everyone Secure

Welcome to the next generation of security.

Ostendio is the only risk management platform that leverages the strength of your greatest asset. Your people. With deep customization, advanced intelligence, and flexible controls, you're always audit-ready, always secure, and always able to take on what's next.

[Schedule a demo today.](#)