CENTRL

THE THIRD-PARTY RISK MANAGEMENT PLAYBOOK

CENTRL

TABLE OF CONTENTS

INTRODUCTION

As companies increasingly rely on outsourcing to reduce costs and enhance the effectiveness of their projects, they face a new class of threats that can strongly impact their reputation, operations, and finances.

Third-party risks are potential exposures that result from a third-party relationship, be it data breaches, non-compliance, or business disruption. And today, managing these risks has become a top priority.

In addition, the pandemic has forced many companies to rely on software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions to migrate their operations to a remote environment. As a result, they are further increasing their dependency on a third-party platform, as well as their risk.

Third-party risk management (TPRM) consists of the assessments, onboarding processes, and risk management tools that can empower an organization to properly combat third-party risk. Its proper deployment can protect your company and its stakeholders from various dangers through a comprehensive enterprise risk management (ERM) program.

WHAT IS THIRD-PARTY RISK MANAGEMENT?

Also known as vendor risk management (VRM), third-party risk management is the process of identifying, assessing, and managing potential risks to a company from its third-party relationships.

A third party is any individual or company outside the management of your organization that impacts your business operations.

Whether data processors, service providers, suppliers, or vendors, third-party businesses can translate into operational benefits or significant risk exposure for a business.

TPRM provides companies with visibility into which vendors maintain information security, compliance, and data privacy standards and which do not.

WHAT ARE SOME OF THE MOST COMMON THIRD-PARTY RISKS?

Organizations rely primarily on third-party suppliers, partners, and contractors to help satisfy consumer needs and keep day-to-day operations running.

Unfortunately, these third-party relationships bring with them significant physical and cyber vulnerabilities that businesses must constantly fight to minimize.

Organizations are frequently compromised due to security flaws presented by third parties that hold sensitive information and access systems or intellectual property. Let's take a closer look at some of the most common third-party risks.

Cybersecurity Risks

Attackers penetrate supply-chain networks, invisibly compromising the systems. The attacker then employs the third party as a "platform" to conduct attacks on higher-value targets.

Through the infected IT infrastructure of your vendors, cybercriminals can execute attacks that facilitate the theft of credentials from your employees or directly from those within the vendor's organization with access to your systems.

Compliance and Regulatory Risks

This sort of risk is frequently caused by a third-party security control failure that results in data loss. Data loss leads to a data privacy breach that exposes the primary organization to repercussions and penalties. Such risks are a significant problem for modern businesses, as 80% of data breaches now involve a third party.

Additionally, third-party violations of environmental or labor laws can also lead to regulatory and compliance risks.

Financial Risks

A third-party activity that harms an organization's financial status is financial risk. This damage might take the shape of subpar vendor work or a faulty component, which slows down company output and decreases income. Penalties and legal bills might also cause financial harm.

Operational Risks

The prospect of a third-party action causing an operational stoppage creates operational risks. A vendor that causes downtime to your organization with late deliveries, poor quality, or system issues introduces operational risks.

Reputational Risks

Negative public opinion generated by security breaches, legal transgressions, or lousy customer interactions creates reputational concerns. When you collaborate with a third party with terrible labor standards or treats its employees unjustly, you put your own reputation at risk.

Strategic Risks

Strategic risk refers to the issues that arise when third-party and organizational business plans are not in sync. This risk is frequently caused by a third party's bad business decisions.

Some third-party risks have a wide range of consequences for enterprises. A data breach is an example of a severe threat that spans numerous risk categories— it interrupts operations, poses a regulatory risk, and results in financial and reputational harm.

WHAT IS A RISK MITIGATION PLAN (RMP)?

Risk mitigation planning is the practice of identifying, evaluating, and selecting solutions to keep risks at acceptable levels within the limitations and objectives of the program. The goal of risk mitigation planning is to ensure the success of a TPRM program.

It specifies what should be done, when it should be done, who is responsible, and how much money is needed to put the risk mitigation strategy into action. Finally, the most appropriate program strategy is chosen from the mitigation strategies and recorded in a risk mitigation plan.

The depth of a risk mitigation plan varies depending on the program's life cycle stage and the nature of the requirement to be addressed. However, there must be sufficient data to give a rough estimate of the work and technological capabilities necessary based on system complexity.

Your RMP will address threats, their possible impact on your operations, and the strategies necessary to mitigate them (avoidance, control, transfer, assumption). The RMP should be reasonable, attainable, quantifiable, and recorded. The following topics should be covered:

- Title of the identified risk
- Plan's date
- Risk owner
- Risk description
- Root causes
- Mitigation options
- Events or activities that could reduce the risk
- Success criteria of the events
- "If successful" value
- Risk status
- Fallback approach
- Handling recommendations
- Appropriate approval levels
- Resources needed

Before an RMP can be created, you must thoroughly understand all potential risks posed by your third-party relationships. You can gain this through the creation of a risk register.

WHAT IS A RISK REGISTER?

The International Organization for Standardization (ISO) definition of a risk register is "a record of information about identified risk."

Risk registers are a risk management tool that employs a risk log to track possible threats associated with a company's activity in general or a specific project. Its goal is to make it easier for risk officers and project managers to monitor potential concerns as they develop and to aid them in minimizing them if they do occur.

These tools can be used manually (through excel sheets and regular updating) or dynamically (via third-party risk management software) to assist risk officers in their mitigation activities.

Although risk registers differ in their purpose or scope, they share specific fundamental characteristics. For example, every risk register should include a risk severity rating based on the chance of it happening and its potential consequences.

This severity rating is based on the company's risk appetite and tolerance and is critical for adequately analyzing possible dangers.

A risk register should also include information on the personnel responsible for each specific risk, depending on the type of risk involved, as well as potential steps to minimize or respond to these risks if they materialize.

The value of a risk register stems from its capacity to consolidate essential information on potential dangers of corporate activities. With a risk register, every risk officer or project team will have all of the information they need to do their job without looking for specific data every time they need to analyze a particular risk.

As a result, resources may be efficiently allocated to minimize the most severe dangers while ignoring minor risks having little influence on the organization or its stakeholders.

Now that you understand categorizing and managing risk, let's cover some best practices when executing your TPRM program.

BEST PRACTICES FOR MANAGING THIRD-PARTY RISK

A company's TPRM program might use a range of best practices. Those shared here have demonstrated the capacity to detect and reduce possible threats over time. They also offer remedial procedures to follow if a data breach occurs.

Here is a summary of some of the best practices to remember when implementing your third-party risk management approach.

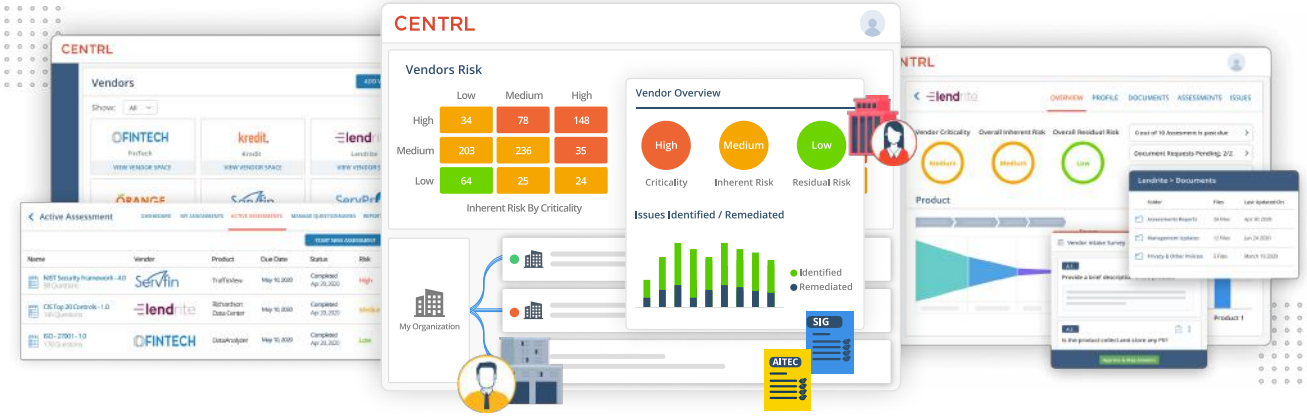
- Before assessing risk, you must first identify all of your third-party partners and understand how much information is exchanged with each. Once you've determined who your vendors are, document what data and networks they can access. Do they require the degree of privilege that they have? If not, you'll have to define some boundaries.
- Requests for proposals must include specific security criteria. In addition, as part of your routine vendor risk management process, employ security questionnaires to zero-in on your bidders' and suppliers' safety requirements.
- You'll want to be able to see which third parties provide the most significant risk to your firm at a glance. Risk ratings can assist you in accomplishing this. Vendors who handle the most mission-critical activities or sensitive data are frequently ranked medium or high.
- Your organization's security team must evaluate vendors, and vulnerabilities must be addressed before exchanging information, data, or goods and services.
- To patch systems for vulnerabilities, software updates must be accessible, and they must be downloaded and installed in real-time.
- Staff should be dedicated to creating, maintaining, and enforcing supply chain physical infrastructure protection and cybersecurity initiatives.
- To mitigate continued vulnerabilities, end-of-life hardware and software should be avoided or must have mitigating measures in place to prevent or limit risk exposure.

HOW CENTRL'S VENDOR360 CAN HELP YOU STREAMLINE YOUR TPRM

TPRM programs evolve as enterprises experience new privacy, business compliance, and cyber risks related to their suppliers. As you can see, the considerations for a robust enterprise risk management strategy are extensive, particularly as your reliance on third parties increases.

The risks vendors pose may not be able to be eliminated completely, but they can be managed, which is vital when relying on third parties.

But to meet these needs as your business scales, along with the number of your third-party relationships, you need an intelligent solution that automates your manual third-party management processes and increases efficiency.



Furthermore, using manual spreadsheets to manage your third-party risks will become unsustainable and unscalable as your business grows. Instead, leaders are turning to third-party and vendor risk management software to streamline and scale their TPRM workflows to keep with the pace of growth.

Vendor360 is a comprehensive and adaptable third-party risk management solution that collects vendor data, automates assessments, and provides you with complete control over your vendor risk management process.

You can use Vendor360 to monitor assessment progress, establish due dates, and check the status of questionnaires throughout your third-party portfolio. The platform also has an easy-to-use user interface, significant automation capabilities, and analytic dashboards.

It can help you speed up pre-contract risk assessment for new vendors by providing questionnaires to several internal teams and monitoring inherent risks at each contractor's engagement, product, and service levels.

Request a demo to discover how Vendor360 can help you with third-party risk management!

CENTRL
VENDOR RISK MANAGEMENT

Learn More: oncentrl.com/vendor360

Get a 1:1 Demo: oncentrl.com/demo-request

US/Global: +1 (415) 780 9667

UK/Europe: +44 020 3037 8609

Australia/APAC: +61 (02) 4910 3822

vendor360@oncentrl.com

/company/centrl

@oncentrl

More Resources

Enjoy this guide?

Visit https://oncentrl.com/resources for more best practice guides, blogs, and ebooks on global bank network management.

CENTRL
VENDOR RISK MANAGEMENT

CENTRL is a leading risk and compliance technology company that provides the most advanced software platform for managing third-party risk and due diligence. CENTRL offers solutions for automating vendor risk management, modern slavery act compliance, operational due diligence, and bank network management. CENTRL's platform is used by leading companies in all sectors across the globe.

US/Global +1 (415) 780 9667 | **UK/Europe** +44 020 3037 8609 | **Australia:** +61 (02) 4910 3822

And, for more information, please visit: oncentrl.com/vendor360

@oncentrl | /company/centrl/

Rev. 2022.01