THIRD-PARTY RISK MANAGEMENT FOR FINANCIAL SERVICES: AN INDUSTRY GUIDEBOOK

CENTRL

THIRD-PARTY RISK MANAGEMENT FOR FINANCIAL SERVICES: AN INDUSTRY GUIDEBOOK

With the increasing adoption of platform, infrastructure, and software-as-a-service tools as mission-critical business applications, running a business without engaging with third parties has become almost impossible.

Third-party providers and vendors greatly benefit organizations by minimizing operational expenses and maximizing process effectiveness. Still, they also bring risks that companies must be aware of to avoid serious consequences.

Third-Party Risk Management (TPRM), also known as Vendor Risk Management (VRM), refers to the group of processes used to identify, assess, and manage potential risks associated with the use of third parties.

As part of a comprehensive Enterprise Risk Management (ERM) strategy, these processes evaluate a business's operations and internal processes, as well as those of any third-party service providers, to identify and mitigate risk associated with the relationship.

TPRM IN THE FINANCIAL SERVICES SECTOR

The financial services industry, in particular, must keep a specific focus on third-party relationships, as risk management and regulation in this industry often has a trickle-down effect in other sectors.

Additionally, TPRM is a critical requirement for businesses that offer financial services to maintain compliance with federal standards from organizations such as:

- The Office of the Comptroller of the Currency (OCC),
- The Federal Financial Institutions Examination Council (FFIEC),
- The Consumer Financial Protection Bureau (CFPB), and
- The Federal Deposit Insurance Corporation (FDIC).

Over the last few years, the financial services industry has incurred the second-highest amount of third-party breaches despite spending over 17,000 hours per year on risk assessments, according to the Ponemon Institute.

With cybercrime on the rise, effective third-party risk management has become more critical than ever and can substantially minimize cybersecurity risks in this sector.

CREATING A THIRD-PARTY RISK MANAGEMENT PROGRAM

Managing third-party risk goes beyond questionnaires and maintaining manual spreadsheets of your subcontractors' and service providers' risk profiles.

Instead, an effective third-party risk management process should take advantage of automation, risk management tools, and continuous monitoring to keep the company in compliance with applicable laws, protect your company from:

- Non-compliance fines,
- Reputational risks, and
- Business interruption.

To streamline these practices, you must clarify each stage that makes up a TPRM program. Generally, the risk management life cycle comprises six stages:

1. Identification of Vendors,
2. Categorization of Vendors,
3. Development of Assessment,
4. Assessment Conduction,
5. Risk Remediation, and
6. Monitoring.

To help you get started on the right path toward a robust TPRM program, we will review these steps in full in the following sections.

Identification of Third-Party Vendors

Ideally, every organization should have an onboarding process that employs due diligence on third-party organizations before initiating any relationship, resulting in a visible and accountable third-party ecosystem. However, if you're starting a new TPRM program, you can begin with the following steps:

1. Contact Accounts Payable and acquire a one-year list of all outgoing payments. We've seen organizations start with a 10,000-line spreadsheet, but after individuals, subscriptions, and single-payment services were removed, they were able to reduce it down to a manageable 400 payee listing within a day or two.

2. Consult the department in charge of legal or contracts for your list to determine whether any third parties have been excluded, as well as whether there are any third parties with whom your business's connection has come to an end prematurely. Your legal team may also assist you in identifying any third parties with which you do or do not have the right to audit.

3. Contact leads and relationship managers after you've finished so that you can double-check and confirm your list.

This will allow you to make a final review of your list of suppliers and service providers, ensuring that it represents the current landscape of your organization.

Categorization of Vendors

Once you have identified all of your company's third-party relationships, you need to know the inherent risks each represents.

Inherent risk is a metric that describes the risk level of an untreated risk, in other words, the associated risk level of a third party without considering any risk remediation measures.

The risk owner should answer a short questionnaire about the inherent risk of the third party, preferably in the form of limited response questions, to reduce the number of possible answers and facilitate the risk assessment.

Some examples include:

- Will the third-party store, transmit, or process any sensitive or regulated data?
- Where will the vendor perform the service? (On-premise, remote, single or multiple locations, etc.)
- What is the concentration of risk regarding this supplier or service provider? (inability to reallocate the activity promptly, limited to no viable alternatives, etc.)
- What is the regulatory compliance risk level associated with the service provided? (High risk: non-compliance with prescribed directives and standards. Medium risk: some concerns by regulators, some risk of non-compliance fines. Low risk: the remote possibility of non-compliance fines)

Selection or Development of Assessment

At this point, you can choose between developing an assessment questionnaire tailored to the specific needs of your company and its risk landscape or implementing an assessment from a risk management standard (such as NIST, ISO, FFIEC, PCI-DSS, CSA CCM, GDPR, etc.).

The most important thing is identifying the controls and questions that provide actionable data. Creating a new risk assessment may be unnecessary when there are several standards available to ensure the effectiveness of your practices.

Vendor360 has several standard templates ready to go, which minimizes the time your risk management team must spend locating and applying a suitable assessment.

Conducting Your Assessment

This step is more than submitting the assessment questionnaires but instead refers to the execution plan and related timelines. It is essential to establish accurate timelines that allow for data collection, identification of risks, and remediation measures.

In addition, the scope of the assessment should be clear, so questions such as "Which products or services are being assessed?" or "Which locations are in-scope?" can help to narrow it down.

Sometimes assessments may only consist of self-assessment questionnaires by your third party. In these cases, you can ask to attach evidence or perform security control demonstrations to validate the accuracy of these assessments.

Although on-site assessments may seem like the ideal option, they are costly and time-consuming and provide little more than a remote assessment, except in cases where:

1. Physical or environmental elements are essential to the assessment, or observation is a regulatory requirement.

2. The third-party wants to maintain absolute control over their data.

3. It is a new relationship or a substantial change in the service provided or the data that is shared

In any case, it is essential to ensure the confidentiality and security of the data provided by your third parties to execute the assessments. Therefore, you should only retain the information provided that is necessary to implement the evaluation.

Address Risks

Once you have completed the assessments, you will need to develop a report with all the information gathered: the third party, the locations and services within scope, the third party's controls vs. the expected controls to protect your company, etc.

The general risk appetite of the company and the risk tolerance of each risk can help you determine the risk remediation strategy of each risk. Your choices are:

- Acceptance,
- Avoidance,
- Transference, or
- Mitigation.

Many risk mitigation measures require working together with a third party to minimize risks, and you should be aware of each measure's physical limitations and time constraints for its implementation.

Continuous Monitoring

As a general rule, third-party relationships are meant to be ongoing, so it makes sense to maintain constant monitoring of the development or progress of your vendors' risk landscape.

No organization remains the same over time, so there will always be changes that will affect your risk rating on your suppliers. Therefore, reviewing the risks and controls of your suppliers is also essential to maintain regulatory compliance.

TPRM BEST PRACTICE RECOMMENDATIONS FOR FINANCIAL SERVICES

Managing the multiple risks presented by third-party relationships in this sector is not easy. Complying with the critical elements of a TPRM program may be insufficient to address the rapid evolution of vendor risks and reduce the effectiveness of your remediation measures.

As your third-party risk management program evolves, you will undoubtedly face resource and timing constraints. Here are some best practice recommendations to help you move your TPRM program forward.

Conduct Ongoing Vendor Due Diligence

To be effective, vendor due diligence must be performed continuously to address all risks and vulnerabilities as they occur.

Due diligence is frequently conducted via third-party questionnaires, which assist financial institutions in gaining a comprehensive understanding of their vendor's environment.

Some VRM tools, live Vendor360, can streamline the due diligence process by giving a shared platform to third parties to update their responses to questionnaires in real-time, removing the need for version control.

Implement Contract-Level Risk Management

Vendor compliance is especially critical in the highly regulated financial services business, where non-compliance can result in considerable financial and reputational loss.

Therefore, when working with third-party suppliers, it is vital to develop compliance rules so that both you and your providers understand how to comply with applicable requirements.
Include performance KPIs in your third-party agreements to analyze third-party security concerning your organization's risk management goals.

By outlining security requirements with your providers, you may build business partnerships based on openness and trust, therefore limiting the effect of possible risks.

Establish Disaster Recovery and Business Continuity Plans

Evaluating your vendor's disaster recovery and business continuity strategies is an essential part of your Vendor Risk Management. You should assess the measures in place for your vendors to maintain their business continuity and if these plans are consistent with your security standards.

It is also critical to discuss your business continuity and disaster recovery requirements with vendors so that they may make necessary changes to their preparations.

Finally, if feasible, include your vendors' business continuity plans into your strategy to simplify review and execution. This also contributes to the efficacy of these strategies by ensuring that specific vendor roles and duties are correctly articulated.

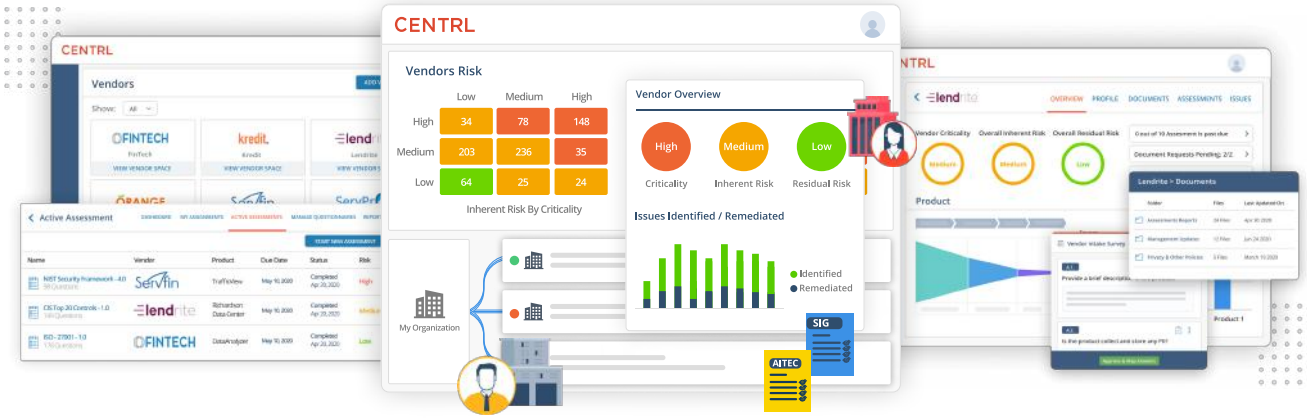
Leverage Automation to Streamline Processes and Stretch Resources

Risk assessment is a time-consuming and complex activity, especially if you have a high number of third parties to evaluate. Automation is one method for addressing both resource restrictions and lengthy assessment timelines.

One simply cannot be aware of every issue that has the potential to damage your third-party ecosystem, no matter how many risk analysts you have on your staff. Fortunately, there are third-party risk management tools, like Vendor360, available to supplement your assessment results and mitigation operations.

In addition, the platform acts as a central repository for all your externally generated data and can help you identify high-risk priorities to focus on first.

VENDOR360 CAN HELP YOU STREAMLINE YOUR TPRM PROGRAM



Managing threats and complying with industry standards is a challenging task. Keeping track of third-party suppliers and the threats they pose to your firm may be too much for spreadsheets or traditional approaches.

However, risk management could be easily achieved by implementing robust third-party risk management software.

Vendor360 is an advanced, customizable third-party risk management platform that collects vendor data, automates assessments, and gives you control over your entire vendor risk management process.

Its capabilities can assist you in expediting pre-contract inherent risk analysis for new vendors by distributing questionnaires to several internal teams and managing inherent risk at each vendor's engagement, product, and service levels.

Vendor360 can also empower you to better monitor assessment progress, establish due dates, and check the status of questionnaires throughout your third-party portfolio, thus relieving much of the burden of manually managing your vendors.

The platform provides an intuitive user experience mixed with extensive automation and analytics to simplify the majority of the third-party risk management process.

To learn more about how Vendor360 can help you streamline your VRM plan, book a demo today!

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