VRM vs. TPRM
VendorInsight
White Paper

MITRATECH

VENDOR RISK MANAGEMENT VS. THIRD PARTY RISK MANAGEMENT: WHAT TO KEEP IN MIND

EnterpriseInsight™

IS VENDOR RISK MANAGEMENT THE SAME AS THIRD-PARTY RISK MANAGEMENT?

Many use the terms vendor risk management (VRM) and third-party risk management (TPRM) interchangeably — but are they the same thing? There isn't a simple answer.

Both terms refer to the process of assessing and managing the risk posed to an organization by outsourced providers. Both kinds of approaches use similar components and common elements from each other. But the truth is they're not synonyms.

Establishing a strong risk management program is an important first step in mitigating risk to your organization. But should you focus more on VRM or TPRM?

WHAT IS VENDOR RISK MANGEMENT (VRM)?

Vendors provide products and services, with well-specified and clearly-defined terms. VRM involves the process of evaluating partners, suppliers, and vendors during the onboarding process and after a contractual relationship is established. A VRM program focuses on the expectations not just for third-party vendors but their own vendors (your fourth-party vendors), and beyond.

VRM's purpose is to ensure the following doesn't develop from a vendor relationship:

- Unacceptable risk of potential business disruption
- Negative impacts on operational performance, such as data breaches
- Violation of regulatory requirements, laws, codes of conduct, or internal organizational policies
- Reputation risk and Environmental, Social, and Governance (ESG) risk

Once risks for each vendor are well understood and controls required to mitigate risks are in place, a company can expand their focus to TPRM.

Examples of Vendors

VRM will use risk assessments to identify and quantify potential risks associated with the use of vendors, such as:

- Companies that sell products
- Consultants and auditors
- Law firms
- Software developers and IT
- Server and website hosts
- Cloud service providers (CSPs)
- Payment processing
- Loan and mortgage origination
- Underwriting
- Business solicitation
- Raw materials provider
- Wire transfers
- Marketing firms

Risk from individual vendors is rolled up and spread across an enterprise to create a risk culture.

WHAT IS THIRD-PARTY RISK MANAGEMENT (TPRM)?

TPRM is broader than VRM and includes every single third party — not just vendors. TPRM is also the preferred term used by the Office of the Comptroller of the Currency (OCC) in the Bulletin 2020-10, the update of the 2013-29 guidelines for risk management. Any organization that requires access to sensitive company data, operations, or finances is a third party.

A TPRM program can start with VRM, but VRM practices can't be applied to all third-party relationships. The major difference between TPRM and VRM is that non-vendor third parties may not have contracts with the organization that is providing them access to data. Consequently, it is difficult to assess and monitor the risks inherent in dealing with these kinds of third parties.

Lacking a direct contract, easy access to documentation, and the ability to audit third parties creates new categories of risk with non-vendor third parties. You lack control and the capability to specify language that requires the supplier to meet certain requirements around:

- Informational, cloud, and cybersecurity
- Operational effectiveness
- Corporate oversight
- Regulatory compliance

TPRM programs, therefore, rely more on monitoring readily available information in the news and on social media. Information can also be gathered by request, such as a regulatory agency voluntarily describing their use of cloud technology.

Contractual language is necessary to reduce risks by ensuring that the controls your vendor has in place are enough to manage risks to your own company. But without a contract and critical access, you need to segue into TPRM practices.

How can your organization make this transition? You need a powerful and user-friendly VRM solution that strengthens your VRM program and helps you to manage certain key activities of a TPRM program.

Examples of Third Parties

While TPRM is unique, it does use VRM as a building block. In addition to vendors, third parties include:

- Business partners
- Venture capitalists
- Regulatory and government agencies
- Franchises
- Non-profits and charities
- Customers

Organizations that start with VRM program can expand the program to address specific and frequently disparate risks from all forms of third parties.

WHAT ABOUT SUPPLIER RISK MANAGEMENT?

Third parties can encompass many things — vendors, contractors, subcontractors, resellers, outsourced providers, merchants, partners, and suppliers. Suppliers specifically provide organizations with goods and/or services, which sounds very much like a vendor.

What's the difference between suppliers and vendors? They can be used almost synonymously, although the International Organization for Standardization (ISO) prefers the term suppliers. A vendor also can refer to both business-to-consumer (B2C) and business-to-business (B2B) sales relationships, but supplier is typically only used for B2B relationships.

This comparison raises the question — what's the difference between supplier risk management, vendor risk management, and third-party risk management?

Supplier Risk Management

Supplier risk management focuses on mitigating supply chain interruptions and reducing risk by addressing supplier-centric risk across the entire lifecycle of a business relationship.

VS

VRM

Vendor risk management deals with vetting partners, suppliers, and vendors by assessing, monitoring, and reporting on risks related to information security, compliance, and more.

VS

TPRM

Third-party risk management can include VRM practices but also involves monitoring third parties who have accessed an organization's data without a contractual agreement.

MANAGE TPRM WITH A POWERHOUSE VRM SOLUTION

When it comes to risk management, you must ask yourself where the biggest risks are coming from — vendors or other third parties. Either way, it always makes sense to start with a VRM program. Building a VRM program will help develop a greater understanding of third parties, and how you can effectively manage them. A solid foundation bolstered by a VRM system will then allow you to extend your risk management into non-vendor third parties.

Utilize a robust software package of functionalities and tools to ensure compliance, assess and report risk, and improve the productivity of your vendor risk management. Once your VRM program is established, a VRM solution can then help you understand the financial requirements, risks, value adds, and challenges associated with different kinds of risk management approaches and program implementations — including TPRM.

You don't have a contract with a third party? Vendor monitoring capabilities give you access to receive risk alerts related to third-party news, financial deterioration, SEC filings, regulatory sanctions, data breaches, and lawsuits. Automated due diligence services monitor social media, abusive practices, and customer complaints and perform Office of Foreign Assets Control (OFAC) screening and watchlist reports. You can receive a complete picture of your third-party risk — vendor and otherwise.

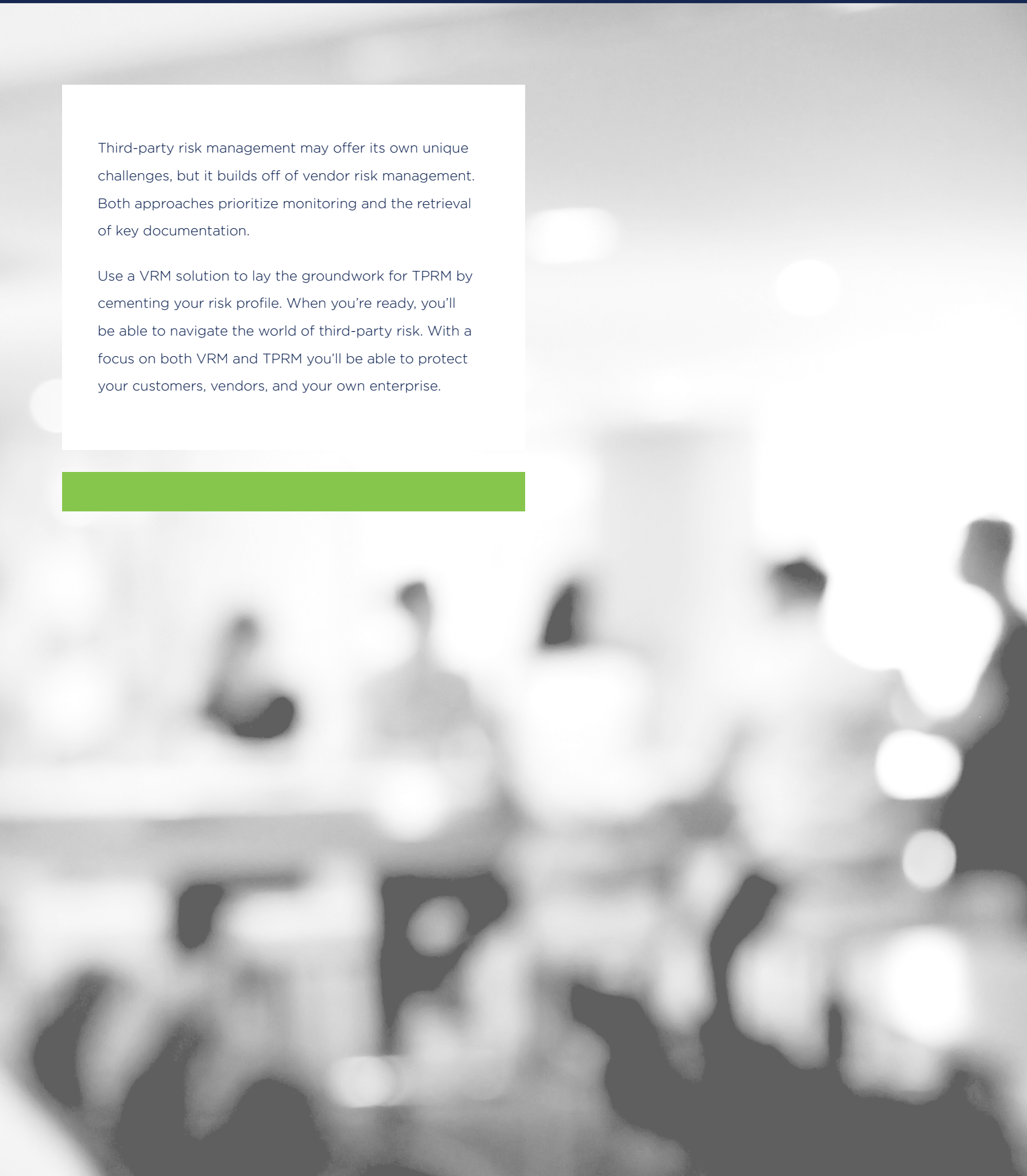
A VRM provider can help in requesting and receiving your third party's private documents under an open Letter of Authorization from you. Those files can be imported automatically or reviewed. Monitoring reports and any documentation voluntarily provided by third parties can then be uploaded into document management functionalities for archival and management purposes.

Find a VRM solution that combines innovative technology and decades of expertise to cover your risk management needs. A committed team of experts and portfolio of capabilities ensure success in the increasingly stringent environment of third-party risk management.

CONCLUSION

Third-party risk management may offer its own unique challenges, but it builds off of vendor risk management. Both approaches prioritize monitoring and the retrieval of key documentation.

Use a VRM solution to lay the groundwork for TPRM by cementing your risk profile. When you're ready, you'll be able to navigate the world of third-party risk. With a focus on both VRM and TPRM you'll be able to protect your customers, vendors, and your own enterprise.



ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk & compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility and spurring collaboration across their organization.

With Mitratech's proven portfolio of end-to-end solutions, organizations worldwide are able to implement best practices and standardize processes across all lines of business to manage risk and ensure business continuity.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com