RISK MANAGEMENT
WHITE PAPER

MITRATECH

MULTIDIMENSIONAL THIRD-PARTY RISK MANAGEMENT

An ABC Guide to Effective Third-Party Risk Management

INTRODUCTION

According to Black Kite's 2022 Third-Party Breach Report the number of third-party data breaches jumped 17% in 2021 compared to the previous year. Ransomware emerged as the most common attack method of third-party related breaches—accounting for 27% of attacks.

The ability to successfully build operational and cyber resilience is a critical component of any organization's need to respond effectively to crises and adapt strategically to change.

Resilient organizations are agile, proactive and collaborative. These qualities are especially crucial in a business environment defined by an increasing interconnection between people, businesses, processes and technology— where uncertainty, risks and potential points of disruption have increased and the accompanying size and nature of their impact is constantly growing.

A core component of operational and cyber resilience, essential to the development of a resilient organization, is without a doubt **Third-Party Risk Management**. It is important to reiterate that resilience is much more than technology, it also encompasses people and processes.

The current business landscape requires proactive, integrated solutions encompassing people, data and infrastructure. Organizations should establish well-defined direction from the top level so that there is clarity on how to act when challenges emerge.

Furthermore, organizations need to move at a rapid pace to deal with risks as they evolve, and this can't be accomplished if risk management is not a priority. New technologies enable organizations with cutting-edge capabilities that encompass data, analytics and modeling. Collaboration is key to achieve smarter processes that will ultimately save valuable time, effort and money.

Working with any third-party vendor or supplier carries an inherent risk. Across industries today, organizations are faced with a two-fold challenge when it comes to managing third-party vendors and suppliers: increasingly stringent regulatory standards on one hand and a simultaneous increase in the complexity of supply chains and delivery models on the other.

Ensuring that third-parties stay compliant is, thus, becoming especially important for businesses trying to minimize risk and achieve greater value by obtaining transparency and standardization in their processes.

Risk management is essential to maintaining operational and cyber resilience in any organization, effective third-party risk management is also required by many of the main industry standards such as ISO 27001, NIST C2M2 and COBIT 5.

At the same time, third-parties might also process or have access to some of your organization's most sensitive data and it is absolutely crucial to know how to approach assessing such third-parties' information security maturity effectively and regularly.

With outsourcing of business processes becoming more common in organizations and to deal with the growing burden of third-party assessments and audits, it is essential to have structured and efficient processes in place.

Needless to say, people form an indispensable part of the equation and they are essential for successful vendor governance and third-party risk management.

EFFECTIVE Third-Party Risk Management

Effective third-party risk management is not something that can be achieved by simply drafting rules or setting up KPIs from an ivory tower..

Each third-party is different — both in terms of who they are as a business, as well as who they are in relation to your business.

To effectively manage these relationships, the Institute for Supply Management (ISM) has identified the following key categories of supplier management activity:

1. Visibility

Gather information regarding the amount of money you spend with each vendor. It is one key indicator to help you establish the importance of said vendor to your business and it helps you identify key suppliers.

2. Vendor Segmentation

This is another useful way to help you understand the relationship between your organization and your vendor. It can also act as a guide for your activities with them.

While most businesses choose to segment their vendors into the 3 categories: **Strategic Key Suppliers, Important Vendors and Tactical Vendors**, it is important that you segment your vendors according to what makes the most sense for your business.

3. Collaborative Attitude

Successful third-party risk management is also about collaboration — sharing information, technologies and open communication. Not only can it create value and cost savings for all parties, it can also help both businesses gain greater visibility and lead to better professional relationships.

4. Performance Management

Managing vendor performance should not merely be about setting KPIs to track performance but about obtaining information with the purpose of improving processes for both sides. The best vendor management KPIs are produced when they are created with input from the vendors as well as agreed upon measures and targets.

5. Risk Management

Effective third-party risk management relies on frequent and comprehensive assessments and is required by many of the main industry standards, including ISO 27001, NIST C2M2, and COBIT 5. At the same time, these should be matched with on- going monitoring activities as well as contingency plans for every risk area that has been identified.

BEST PRACTICES IN Third-Party Risk Management

1. Define a Clear Set of Controls.

Defining a set of controls for an assessment template is the first step in streamlining your third-party risk assessment process. It is important to define a clear set of information security controls that you would expect your third-parties to satisfy. The controls should then be turned into a template assessment to be sent to vendors during due diligence and audits.

The controls should cover a sufficient range of topics to allow you to identify any risks that might exist. Some key topics might include: identity and access management, physical security, security monitoring, cryptography, and business continuity management.

Controls and assessment questions for testing those controls should be specific, direct and close-ended. Rather than asking general questions, ask the vendor directly whether it exercises key controls that you would expect a third-party to have in place. Such questions will be easier for the vendor to answer and the completed assessment will give you a clearer indication of the vendor's cyber maturity, requiring less emails and spreadsheets back and forth.

2. Automate Third-Party Assessments

If done manually, assessing your organization's third-parties will eat up excessive resources and be extremely time consuming and painful. Wherever possible, the assessment process should be automated in order to save resources and time, reduce human error and obtain deeper risk insights.

3. Vendor Conflict Check

Before signing a contract with a third-party it is best practice and often a legal requirement for an organization to ensure that a conflict of interest does not exist. The organization must be sure that a conflict does not exist between the vendor's own interests and the interests of the organization.

As part of this process, it is common to make sure that no circumstances exist where engaging the vendor would in any way harm the organization.

As a first step, each organization should identify a list of scenarios in which a conflict of interests would be likely to exist or where entering into a relationship would be detrimental to the organization. Some examples of risk indicators might be:

- Where a member of the organization is an owner of or holds a direct financial interest in the vendor.
- Where engaging with the vendor might violate legal restrictions or sanctions against countries.
- Where fraud or corruption charges have previously been levied against the vendor.
- Where benefits or gifts have been exchanged between the parties.
- Where the vendor relationship is likely to cause negative media exposure.

In order to ensure operational resilience, it is essential that each third-party is subjected to a rigid and thorough vendor conflict check, with deeper examination and assessment of riskier vendor relationships.

SUCCESS FACTORS IN Third-Party Risk Management

1. Build Strategic Partnerships

The most effective TPRM strategy is one that focuses on picking the right vendors and is directed towards forging mutually beneficial strategic partnerships with them.

2. Limit the Number of Third-Parties

It is difficult to invest time and resources building strategic partnerships if you have too many vendors providing similar services. Focus on a smaller number of firms and establishing great relationships with those select few.

3. Open Communication

Once you've picked your strategic partners, it's all about communicating openly and truthfully. Discuss performance issues openly and give them a chance to solve those problems before jumping to replace providers. Remember, good relationships are difficult to replace.

BUILDING A Third-Party Risk Management

Being able to have a 360 degree risk view of your organization's third-parties is key to achieve a fully holistic Enterprise Risk Management (ERM) lifecycle.

Aim for the following in your TPRM framework:

1. Configure your TPRM Workflow

Start with all required vendor governance workflows that follow your organizational processes. Categorize your vendors by risk exposure and other criteria to fully refine your analysis.

2. Gather Data

Gain data and information on your vendors through security performance indicator platforms like SecurityScorecard. Filter and sort your vendor portfolio based on security criteria in real-time.

3. Launch Assessments

At scale assessments provide a detailed analysis of your vendors. Make sure you are asking the right questions and getting meaningful answers in compliance with relevant standards, laws and regulations.

4. Analyze Maturity Details

Advanced analytics enable you to pinpoint uncertainty in performance and potential sources of risk in assessment responses, as well as automate risk identification and qualification.

5. Benchmark and Aggregate Vendor Portfolio

Analyze similar data points and compare or aggregate results. Benchmark vendor cohorts in the context of standards, laws and regulations.

6. Continuously Manage Vendor Risk

Integrate vendor insights into your Enterprise Risk Management (ERM), by executing the full risk lifecycle of your vendors, from status and review workflows, on an asset or portfolio basis.

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk, and compliance professionals seeking to maximize productivity, control expense, and mitigate risk by deepening organizational alignment, increasing visibility and spurring collaboration across the enterprise.

With Mitratech's proven portfolio of end-to-end solutions, enterprises worldwide are able to implement best practices and standardize processes throughout their organizations and realize fast time-to-value.

Serving 1,200 organizations of all sizes worldwide, Mitratech works with almost 40% of the Fortune 500 and over 500,000 users in over 160 countries.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com