BLACK KITE

THE ULTIMATE GUIDE to Building a Third-Party Risk Program

2023 OPERATIONALIZATION GUIDE

TABLE OF CONTENTS

We know that managing third-party risk is important. But how do you put it into practice?

Introduction to Third-Party Risk Management

Third-party risk management strategies haven't changed much in the past 20 years, but the third-party risk ecosystem has. Consider this: Today's organizations, on average, have anywhere from 20 to 50 vendors. Some are connected to as many as 200, and they're not all software vendors. Any and all types of vendors introduce risk.

Despite this vendor boom, most organizations still rely on manual questionnaires to assess and determine vendor risk. While simple questionnaires might've worked well 20 years ago, they hardly paint the full picture of risk to organizations today.

The impact? According to the Verizon Data Breach Investigations Report, 62% of system intrusion patterns in 2022 involved a compromised partner. Our 2023 Third-Party Breach Report found that third-party incidents affected 4.73 organizations per compromised vendor.

That's the cascading ripple effect of poor risk assessment strategies. Even if you weren't the one initially compromised, you still might become a bad actor's next target.

Considering the average cost of a data breach reached $15.01 million in 2022, security professionals must adapt their third-party risk management (TPRM) programs — or risk losing time, money, and a good reputation.

The threat landscape is more diverse, active, and interconnected than ever — and that means third-party risk management policies should be top of mind for today's security leaders. However, the number and magnitude of third-party breaches today also indicate that protecting digital supply chains is a tough task to handle, especially when most organizations are relying on old-hat methods.

What's the major problem with the current approach to TPRM? **It's qualitative, not quantitative.** That makes putting a TPRM program into practice a massive struggle. In this guide, we'll dive into the top five steps to building out a modernized third-party risk management program.

Challenges Facing Third-Party Risk Management Programs

Have you ever heard the phrase: “Do more with less?” Imagine that on steroids, and you’ve got the essence of what it’s like to run a third-party risk management program.

It’s a tale as old as time: TPRM pros need to adapt their programs and policies to the horde of new vendors in their networks, but they can’t ask for more budget, time, or resources. They have to “do more with less.”

Why is securing more budget and resources such a hard ask for security teams? It’s because investing in tech is more costly than ever.

Gartner predicts that IT spend will reach $4.5 trillion in 2023 — a 2.4% increase from 2022. That’s already a lot of pressure on company wallets, hence security pros being tasked to “do more with less.”

This is especially true during economic uncertainty — which tends to make already financially conscious stakeholders even more spend-shy.

That “do more with less” mentality can cause a domino effect of challenges to implementing an effective TPRM strategy — for a number of reasons.

QUESTIONNAIRE OVERLOAD

Security teams are pushed to improvise when it comes to doing more with less. How is that usually interpreted? By creating (and sending out) even more questionnaires.

Because of tight budgets and limited resources, it can be challenging for security teams to pursue risk assessment methods beyond questionnaires. Questionnaires are already a well-established and cost-effective strategy, so organizations continue to rely on them.

Vendors can feel overwhelmed by an avalanche of questionnaires and will try to answer as optimistically as possible.

Those overly optimistic answers can lead to a picture of risk that isn’t totally accurate. What one vendor considers “good” or effective security performance may not be the same for another vendor or organization.

Here’s the major problem with questionnaires: They’re usually designed to get qualitative data. That can make it difficult to develop a consistent way of measuring risk across vendors. Those qualitative answers can create a skewed view of the risk attached to them. Which then leads to security surprises down the road.

Challenges Facing Third-Party Risk Management Programs

NO INCIDENTS = STRONG SECURITY? NOT NECESSARILY

As far as most organizations are concerned, questionnaires have "worked" so far — in that they provide some type of security insight. That "if it ain't broke, don't fix it" mindset can prevent internal teams from building out a TPRM program.

Think of it this way: If you're walking around the woods carrying around pounds of raw meat and a bear doesn't attack you, does it mean that you're safe from a bear attack? Chances are, no. It just means that you happened to get pretty lucky.

Just like the risk of a bear attack in the woods, the risk of a breach when working with third parties is always there. According to Dark Reading, 98% of organizations work with a vendor that has already experienced a breach or incident. That means that most — if not nearly all — organizations face a high risk of third-party attacks.

WHAT'S THE KEY TAKEAWAY HERE?

Just because a vendor hasn't been breached yet doesn't mean that their security program is up to par. And it doesn't mean that a potential breach of a vendor wouldn't pose a serious financial risk.

This outlook of "It hasn't happened *yet*," can prevent teams from implementing a proactive TPRM program in favor of reactive (and highly risky) policies.

FIVE STEPS TO BUILD A MODERN TPRM PROGRAM

Modern challenges require modern solutions.

Here are **five steps** that organizations must take to build out a TPRM program that effectively mitigates vendor risk.

Step One: Determine Your Vendor Scope

The first step in building a TPRM program is to determine which vendors to focus on and track. Establishing this scope sets your program up with boundaries that can help keep excessive pressure off teams to closely monitor all vendors.

Essentially, the first thing that organizations need to understand is which vendors in their vendor ecosystem: **have access to their data, process their data, have access to systems that have their data, or even have access to their systems in general.**

It is important to go beyond just knowing merely who is handling your data and where. Identifying all types of significant connections is just as important.

Why? Because bad actors are no dummies. If they can breach one system, they can quickly find ways of breaching others — even those that are seemingly unrelated.

While determining vendor scope, be sure to consider materiality. How important is that vendor to business operations?

How would it materially affect business if something occurred to that vendor? If any breaches, leaks, or incidents would affect business significantly, then those vendors need to be included within the TPRM scope.

TO FIGURE OUT WHICH VENDORS REQUIRE GREATER ATTENTION AND WHICH NEED LESS, ORGANIZATIONS MUST ASK:

What risk does this vendor pose to my organization in particular?
What kind of risk or risk scenarios could happen while working with them?

Step One: Determine Your Vendor Scope

Answering these questions not only helps security teams hone in on where threats are most likely to happen — it also saves the whole organization a lot of time and resources. Instead of getting bogged down by alert fatigue because teams are monitoring for every little hiccup, they can zero in on threats where they really matter.

Once organizations determine the scope of their vendors, where should that scope live? Ideally, they should have an internal database of all vendors of interest — and that database should be directly fed into their TPRM platform.

REDUCING UNCERTAINTY ABOUT THE RISKS YOU HAVE

Here's the key to reducing uncertainty about risk: Separating acceptable from unacceptable risks.

What determines acceptable risk? It comes down to weighing costs against benefits. If a third-party vendor saves your organization $12 million a year but has a potential $20,000 in risk attached to it, then that's a risk that your organization will likely be willing to take.

Now imagine a third-party vendor — with the same risk letter grade — saves your organization $100,000 a year but has a potential $13 million in risk attached to it. The costs clearly outweigh the benefits.

That's why quantitative, not just qualitative, data is so important in third-party risk management. It concretely illustrates what the risk means so that you can make better-informed business decisions.

Keep in mind that acceptable risk is determined by your organization's own risk appetite. What might be a small incident for one company might be completely devastating for another.

That's why it is critical to establish (in concrete, financial terms) what your organization is willing to lose — and what it's not.

THE BLACK KITE DIFFERENCE: TRIAGING

With Black Kite, you do not necessarily need to examine every vendor your company deals with. Instead, you can build a Black Kite-specific database that includes the vendors that match your organization's risk appetite.

These criteria might include whether or not a vendor has access to your data, processes data, or manages sensitive data. Once you've established which vendors you want to monitor, you can then triage the vendors that present the highest probable financial impact.

Black Kite has a sortable column header organizing probable financial impact from highest to lowest. That way, you can identify vendors that fall significantly above your risk tolerance.

Step Two: Identify Specific Risk Scenarios

Once organizations identify the global pool of vendors within their TPRM scope, they should then move on to identifying specific risk scenarios — or real-life incidents — to concretely quantify risk.

How do risk scenarios lead to quantified risk? Many TPRM programs opt for rating vendor risk in grades — but it's hard to quantify risk with grades. Grades and ratings generally assess the security prowess of vendors, which can definitely be helpful in getting a general ballpark for risk.

But grades cannot account for every single detail. When it comes to third-party risk, those details can make all the difference.

Organizations must take real-life examples, identify where and what they might stand to lose if those scenarios occur, and then find the range of money that's at stake.

They cannot simply rely on ratings and grades alone because they don't address the practical issue at hand: **What would the probable financial impact be if one of these vendors got breached?**

WHEN BUILDING RISK SCENARIOS, ORGANIZATIONS SHOULD CONSIDER THE FOLLOWING:

- ***Natural disasters (e.g., hurricanes, tropical storms, earthquakes)***
- ***Geopolitical conflict (e.g., embargoes, sanctions, war)***
- ***Digital developments (e.g., new ransomware, CVEs, patches)***
- ***Regulations (e.g., HIPAA, GDPR)***

WHEN BUILDING OUT A TPRM PROGRAM, ORGANIZATIONS MUST CREATE RISK SCENARIOS THAT ARE SPECIFIC AND DETAILED.

Step Two: Identify Specific Risk Scenarios

Let's dive into this a little bit more with an example risk scenario.

Say that your organization is doing business with a call-center vendor based in the Caribbean. What would the financial impact be if a hurricane hit the vendor's headquarters and stopped the call center from being able to support calls for a period of four months?

That same level of detail applies to creating cyber risk scenarios. This is where all that groundwork laid during step one comes in handy.

When an organization knows when and how vendors come into contact with their data, they can derive what scenarios are most likely to happen — whether that's an exploited software vulnerability, a ransomware attack, or a phishing attempt.

Building out the right risk scenarios starts with knowing where your organization's most valuable assets lie and where an attack would hurt the most. Then, teams have enough starting ground to identify which vendors might impact them the most.

THE BLACK KITE DIFFERENCE: COMPLIANCE FRAMEWORKS

GDPR, in particular, can be a difficult regulatory body to navigate. When you're operating under the auspices of GDPR, you have to make sure that your vendors are also operating under those rules. What would happen to your organization if it was subjected to a GDPR fine? Creating a risk scenario based on that question can help you ultimately determine whether a vendor is worth doing business with or not.

With Black Kite, highly regulated organizations can factor compliance into risk with ease. Our Compliance Module includes well-known industry standards (like GDPR, NIST, and HIPAA) as well as the ability to upload and map customized frameworks to your vendors. Simply click on the Compliance Overview tab on each vendor to see how they measure up.

Step Three: Calculate the Financial Impact

With those specific risk scenarios, it's time to dig deep and quantify vendor risk by calculating the potential financial impact linked to each risk scenario. This is the real "risk" part of third-party risk management.

How can you determine what an incident with a vendor might cost your organization? Identify what data they have access to and what resources of yours could possibly leak or become breached.

Then, organizations can create risk scenarios around threats to that data and project a range for the financial cost of that breach.

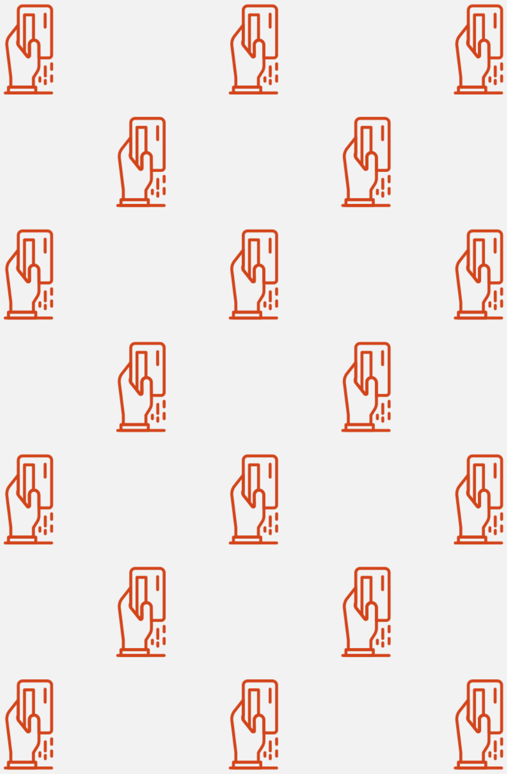
Next, organizations should rank vendors by probable financial impact — not just their risk ratings or letter grades.

THE LIMITATIONS OF RISK RATINGS

Why should organizations focus on probable financial impact instead of risk ratings? It's because these ratings don't always paint the full picture when it comes to risk.

For example, look at the 2021 Colonial Pipeline breach. While the Colonial Pipeline had a decent security rating, those ratings could not account for the fact that Colonial Pipeline credentials had already been leaked onto the dark web.

Bad actors then took those credentials and started credential stuffing until they were able to breach Colonial Pipeline's systems.



Step Three: Calculate the Financial Impact

Identifying probable financial impact is one of the soundest ways to conduct a risk assessment. It shows you specifically which vendors, if compromised, would deal the biggest blow to your organization — and which would deal the smallest.

This step can also help overcome challenges in illustrating risk to stakeholders and key decision-makers.

Communicating that a vendor poses a $10 million risk to your company is more tangible for stakeholders than telling them a vendor poses a "high" risk or has a "C" letter grade.

When stakeholders have a number related to probable financial impact in front of them, they can determine whether or not it's a number that they're willing to risk losing.

That not only helps **unlock better business decisions** but also helps communicate the value of a strong TPRM program to your board.

THE BLACK KITE DIFFERENCE: FINANCIAL IMPACT SOURCING

Black Kite's platform shows you the financial impact your vendors can have on your organization if breached. With Black Kite, you can also view each vendor displayed as "high financial impact" from the ecosystem list.

Exclamation marks on financial impact indicate that these figures have been derived from industry sources. To get an even more accurate estimate, you can update the number of your records exposed to the vendor.

Step Four: Apply Resources to the Highest Risk Vendors

– Ask Questions, Assess, and Automate

Notice how we said highest risk, not highest priority vendors. Cybercriminals aren't concerned with how critical a vendor is to your organization. They care about how easily they can hack it.

Once organizations know which vendors could cause the greatest impact if breached, they can focus their team's resources.

That last step can get a bit tricky. To properly elevate your TPRM program, it is key to only automate processes that are actually valuable to your organization.

For example, let's say you have artifacts you've collected from a vendor. If you can automate the analysis of those documents that show you where the gaps in their security program are, then you have a useful automated process.

ORGANIZATIONS CAN THEN PROCEED BY:

- ***Sending risk assessments and questionnaires to their highest-impact vendors, helping teams hone in on the right data they need to build out risk scenarios.***
- ***Leveraging automation as their TPRM program's best friend.***

By contrast, simply automating the process of sending out those questionnaires to your vendors isn't necessarily helpful — nor does it guarantee that it will improve your ability to evaluate risk.

THE BLACK KITE DIFFERENCE: AUTOMATION

Black Kite builds out your TPRM program by leveraging the right kind of automation. The Black Kite platform automatically discovers relevant data to your vendor ecosystem and presents a comprehensive view of the financial risk posed by each vendor.

How does Black Kite do this? By continuously monitoring and keeping tabs on those vendors for risk updates or changes — and automatically notifying teams of significant changes, stat. With automation in place, you've not only unlocked the data you need to be more confident in your results, but you've also freed up your team to focus on another key component of operationalization: *monitoring for changes.*

Step Five: Monitor for Changes

The fifth step in building out a third-party risk management program is to continuously monitor for changes that might require teams to take action.

The key here is to identify changes that will *actually* affect an organization. If vendor changes have no bearing on business functions, then they're not changes worth tracking. In fact, monitoring for *those* changes will only cost you much-needed time and resources.

What's an example of a change that *doesn't* necessarily matter? Patching levels. Twenty years ago, those were a key metric for determining the security of an organization's systems. Nowadays, patching happens so frequently that increased or decreased levels don't necessarily tell you anything about a vendor's security posture.

If companies do notice a change, they can then re-assess the risk related to working with that vendor. That new information could make or break the chance of becoming the next target of a third-party breach.

SO, WHAT *SHOULD* ORGANIZATIONS LOOK OUT FOR?

- ***Severe security rating downgrades and drops.***
- ***CVEs that bad actors are frequently exploiting in the news.***
- ***Significant geopolitical shifts.***
- ***New data being shared with vendors and how it's being shared.***

THE BLACK KITE DIFFERENCE: CONTINUOUS MONITORING APPROACH

Listing continuous monitoring as the last step is a bit of a misnomer. In reality, continuous monitoring should be more of a cycle — something that is done *consistently* and *continuously*.

Black Kite places continuous monitoring at the forefront of the operationalizing process. It is both the first and last step in the TPRM process. This approach outlasts the rest because it is consistently forward-thinking. Instead of reactive, it's **proactive** — a key trait security teams must adopt if they aim to stay ahead of bad actors.

The Foundation of Operationalization: **Quantitative Data**

The threat landscape is in a constant phase of metamorphosis. To build a TPRM program, it must have a foundation that is adaptable to (and conscious of) that change.

A robust TPRM program is about understanding these changes in the context of the total risk posture each vendor presents.

ORGANIZATIONS CAN SUCCEED IN MODERNIZING A TPRM PROGRAM IF THEY:

- ***Identify their vendor ecosystem correctly.***
- ***Develop the risk scenarios that are important to the organization.***
- ***Pinpoint the quantitative risk of those scenarios with potential financial impact.***

Remember, it's about *quantitative*, not qualitative data. Once organizations have all the right data, then they can make those critical business decisions — and reduce the uncertainty around what the *impact* of third-party risks will be.

Automation tools make up the backbone of a robust TPRM program. The Black Kite platform thrives on automated processes meant to make risk assessments more accurate, efficient, and actionable. Take your TPRM to the next level — get in touch with Black Kite today.

GET IN TOUCH