THRIVE THROUGH TRANSFORMATION

BITSIGHT
The Standard in SECURITY RATINGS

EBOOK

3 Ways to Make Your Vendor Lifecycle More Efficient

INTRODUCTION

Third Party Risk Management is full of difficult decisions. As the world adjusts to the "new normal" brought on by COVID-19, Third Party Risk Management (TPRM) teams are being forced to reckon with an entirely new reality. Businesses are bringing on vendors faster than ever before, and doing so at a speed that is unprecedented. Meanwhile budgets across the board are shrinking, as are headcount numbers. That means that TPRM teams are under immense pressure to onboard more vendors faster and with less cost.

Bringing on a new vendor might seem simple: You just pick a vendor with the right capabilities and the right price and get the paperwork signed. But those who have to manage third party risk know that it's rarely so simple. That's because Third Party Risk Management is a complex task that is full of difficult decisions and requires cooperation with multiple business departments like legal, procurement and finance, as well as the hard work of assessment and onboarding the vendor and managing them over the course of the vendor lifecycle. The challenges of COVID-19 and the transition to a work from home environment has only made things more difficult.

But the disruption to normal operations can be something of a blessing in disguise. It's an opportunity to rethink the way you run your program.

As you think about your TPRM program, **ask yourself these questions**:

1. Are you doing things the way you are because you've always done them that way?
2. Are you having difficulty adapting your program to the work from home world?
3. Are there opportunities to make your program more efficient or reduce cost?
4. Is your program struggling to approach TPRM from a business enablement perspective?

If you've answered yes to any of them, then it's probably time to rethink the policies, processes and communication strategies for your TPRM program.

Here are three critical stages of your program that may be ripe for a revamp.

1. SECURITY PROGRAM POLICIES

In our current climate, the need to manage vendor risk is colliding with work-from-home employees trying to adjust to new circumstances. To enable those employees, businesses are bringing on more vendors, and expect them to be onboarded quickly. But how do you enable the business unit leaders to help you help them?

The quick answer lies in the policies you have in place. When the right policies are in place from the start of the vendor procurement process, all the way throughout your relationship with outside parties, security leaders are able to efficiently manage their programs. Dictating ownership and communicating timelines to all those involved is easier to follow when policies are set-in-stone. Let's dive into the details of policies, and how prioritizing policies in third-party risk management will solve a multitude of problems for security leaders.

Enabling Your Business During Procurement

One of the most critical points in your relationship with a third-party is during the procurement process. You want to have an organized approach to initiating relationships and evaluating third parties so that the best vendors will want to work with you.

During the procurement phase, there are three areas you can optimize your policies to run your TPRM program more efficiently:

- Have you set policies about **security criteria** for vendor selection?

Having a standard, consistent requirement of what you need from a third-party in terms of their cybersecurity programs is important when considering a large pool of vendors. It is much easier to narrow down to the specific third-party that meets your security requirements when using a rating system like BitSight for Third-Party Risk Management. Business unit leaders can help the third-party risk team limit time spent analyzing vendors when they are aware of the security criteria. The transparency between teams can lead to collaboration earlier in the vendor selection process, and vendors can be submitted for security rating analysis and approval before the business unit is invested in the partnership.

- Have those policies been crafted in **collaboration with procurement, legal, and finance?**

To make sure your policies are properly reflecting the goals of everyone in your organization, it is important to craft these security policies in collaboration with departments such as procurement, legal, finance, and compliance. Including your legal team in cybersecurity policies will help you avoid any legal confusion and make sure contract wording is ironclad and makes the TPRM process enforceable. Involving the procurement and finance departments will help you determine your budget prior to meeting with third-parties, and involving compliance can help ensure that the vendor is able to meet any regulatory requirements.

- Have those policies been communicated to the **functional business unit leaders** and socialized with the managers?

While they might not be involved directly in each vendor selection conversation, it is important to communicate your selection and procurement policies to the leaders of each business unit within your organization. Ensuring policies trickle down to the leaders and managers of individual teams will make your vendor procurement process more efficient and top of mind in manager's decisions. Business managers have to be mindful that their vendor selection ultimately can impact the over business reputation and success, so considering security standards and policies is key.

Business managers have to be mindful that their vendor selection ultimately can impact the over business reputation and success, so considering security standards and policies is key.

Building Bridges To Create Security Partnerships

Diving deeper into creating cybersecurity policies that work across the business entity, it's important to prioritize transparency between the security team and the rest of the business. Frustrations can arise surrounding third-party risk management when responsibilities and processes are roadblocks for the business. Having clear and agreed-upon policies to apply to every vendor onboarding experience can begin your relationship with your new third-party in a positive way across the board.

A great example of an easy-to-apply policy to use to streamline the vendor onboarding process is to set a minimum rating required for vendors to be considered by your organization.This will help align all departments and allows business units to prescreen their list of potential vendors prior to an in-depth assessment from the procurement and security teams. This will not only prioritize the most secure vendors but should lead to fewer big surprises down the road in the vendor relationship.

BitSight for Third-Party Risk Management can assist with the prescreening step of the vendor selection process by providing the third-parties' cybersecurity rating, calculated objectively based on public website and security information. The scoring policy does not require excessive time and effort from security or procurement teams because it is calculated in the BitSight database, and considers 23 common security measures for each vendor.

Use Of Policies Throughout The Entire Vendor Lifecycle

We described in detail how important it is to implement efficient policies during the procurement and onboarding stages of the vendor lifecycle, but it is important to consider where else in your third-party risk management plan you can implement more efficient policies.

Implementing the right policies during the assessment phases of your program can also help scale your program to meet your growing number of third-parties. Traditionally vendor assessment occurs in a yearly cycle where a third party's processes are re-evaluated to make sure they have maintained their security standards. Oftentimes organizations face an overwhelming number of vendors to evaluate at one time, and might not be evaluating vendors as in-depth as they wish they could.

Yearly assessments only capture a snapshot of a vendor's cybersecurity status, which might not paint the whole picture for how a vendor has performed throughout the year. To best manage a vendor's security risks, any adverse cyber event should trigger a vendor assessment, including things like a large drop in their security rating or an increase in risk vectors.

Use of the right policies will provide crucial transparency to all those involved in a vendor relationship. If, for example, you set a policy so that your most critically tiered vendors are evaluated yearly and your lower-tiered vendors are reassessed only when security threats arise, you are setting clear expectations between your vendors, your internal parties, and the security team.

2. MAXIMIZE EFFICIENCIES WITHIN THE REASSESSMENT PROCESS

Your third-parties may be deeply integrated within your data and systems after onboarding, and any vulnerabilities in your vendors will result in a threat to your systems as well.

What Are Most Companies Doing?

Many companies follow a basic outline for reassessing their vendors based on their budget. Security leaders frequently use the same assessment measures, questions, and techniques when analyzing all of their vendors, independent of the vendor's use-case or level of criticality with the organization's function. While distributing the same assessment across your entire pool of vendors initially seems like the most efficient way to do things, it actually creates additional, unnecessary work for both vendors and TPRM program teams.

The third-parties that are partnered with your organization to help with the more remedial, operational tasks might be overwhelmed with a vendor assessment that takes them weeks or months to complete. On the other hand you might be missing a key piece of information about their cybersecurity health for your most critical vendors if they are given a less-lengthy standard assessment. So how can you make your reassessment process more efficient?

Outperform The Rest

By using a more tailored approach to handling critical vendors, combined with monitoring methods that detect threats immediately instead of once a year, security managers can regain an efficient vendor assessment process.

Tiering: Mitigate Risk Where It Matters Most

One of the best ways to optimize efficiency while mitigating risk is by tiering your vendors. Tiering involves breaking your third-parties into sub-categories based on their level of criticality and security performance. Vendors that work heavily with your most secure data or processes can be placed in a higher, more critical tier. Vendors who hold less inherent risk, and who have a secure historical performance when it comes to risk management fall into a lower tier.

The BitSight Tier Recommender can provide intelligent recommendations for which tier a third-party falls into based on their historical security performance, as well as their use-case within your company's operations. If a vendor has a stellar performance record and is determined to be of tier 3 importance, your cybersecurity team can spend less time and money evaluating that vendor each cycle. Third-parties with high, tier 1 importance, and who have a riskier historical cybersecurity performance will require a deeper dive for their reassessment. A vendor's historical performance and program trendline can help you determine the level of assessment they need without taking the chance that a third-party is over-promising their security measures early on in your partnership.

Don't take the chance that a third-party is over-promising their security measures early on in your partnership.

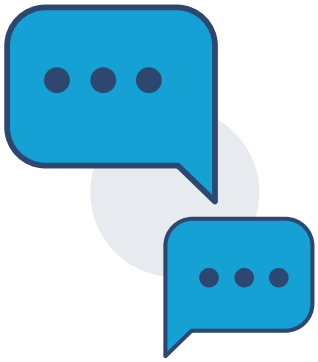
Continuously Monitor Your Third-Parties For Changes In Security Status

Where implementing a tiering system helps prioritize *how* you evaluate vendors, we can also make the process of *when* you evaluate your vendors more efficient by focusing on a continuous monitoring system.

Continuous monitoring involves consistent observation of a vendor's cybersecurity program so that instead of waiting to analyze the malicious activity happening within your third-party's system on a yearly basis, you are immediately notified when dangerous activity occurs. If a continuous monitoring system is in place, your organization can resolve the issue before you are even contacted by the third party themselves.

You can also set risk thresholds so that when an outside party experiences a drop in their risk management score to a level your organization is not comfortable with, a reassessment trigger can notify your organization's security team. If a vendor has maintained a consistent cybersecurity score throughout a given period, or if their score has actually risen, they might only need a lighter assessment or a simple health check of their systems.

Using continuous monitoring technology like the BitSight for Third-Party Risk Management platform gives you greater control over where and how your time and money is spent on managing your third-parties. By using BitSight's tiering technology, you can confidently decide which vendors to push more resources towards, and then continuously monitor security ratings to better prepare and react to cyber threats.



3. SUCCESSFULLY COMMUNICATING RISK

While finding and implementing the efficient processes are crucial to successfully onboarding and overseeing your third-parties, the hard work can be lost if there is a disconnect with your executive leadership or board. Focusing on communication cannot be stressed enough when it comes to demonstrating the work of your security team.

The list of stakeholders that should be involved in cybersecurity conversations can include senior leadership, board members, business partners, and at times your investors. Each stakeholder might have different levels of understanding when it comes to cybersecurity, so you can't discuss your program and metrics the way you're familiar with. Senior leaders are involved in the decisions regarding headcount and budgeting for TPRM teams, so finding simple and effective communication techniques that work for your leadership group is important to make sure your team is receiving the resources you need.

Where Miscommunication Leads To Gaps

When working consistently within the third-party risk business it is easy to forget how confusing security metrics can seem. TPRM leaders often rely too much on technical terms and jargon when presenting their security data to the board, which can lead to frustration. If the security team doesn't pay attention to this, it can create a divide from the leaders they are hoping to gain support and resources from.

Another common area of miscommunication that can lead to tension between a security team and their board members is when there is limited-to-no context given on information presented. For most business departments, the board is familiar with what they are referring to because most company executives have worked with statistics involving retention rates, return on investment, cash flows, etc. For security professionals, the board is probably not sure of how these specific metrics are impacting business performance overall.

How To Fix Miscommunication

So how can cybersecurity professionals avoid the negative impacts of miscommunication when interacting with the company stakeholders? Taking a step back from the specifics of how their cybersecurity efforts are performing at the detailed level, TPRM leaders need to connect their team's initiatives back to how they impact the organization's goals as a whole.

For example, presenting a slide to the board showing a vendor's specific security rating, along with the specific malware found in their footprint might seem like a clear and concise description to a security leader, but could fall beyond the understanding of the board. BitSight's TPRM platform includes a Risk Communication feature that helps security teams explain what a risk vector is to those that aren't working with cybersecurity day-to-day. The tool can also provide context to what metrics means to your security profile as a whole, providing key contextual information. It is important to convey the valuable ways managing third-party risk is enabling the overall business to stay competitive and innovative by displaying the security information in terms that relate to the company goals.

Providing The Right Context

As mentioned briefly before, contextual details behind the information you're presenting to the board is key to ensuring that the information is understood and applied correctly in the decision-making process. It can be helpful to include contextual information like:

- How a vendor ranks compared to an **industry average** instead of blanket vendor security scores with nothing to compare them to.
- Details around the **company policy** for minimum scores allowed by your vendors. It can be helpful to show where your vendors, especially the most critical ones, fall compared to where the company requires them to be.
- If a vendor has a dip in their score, is this representative of their **historical performance**?
- A general, **high-level overview** of what actually occurs during the malicious activity in question can help set the scene for what happened to cause a vendor's score to dip. Be careful to avoid over-using cybersecurity jargon that will confuse those not familiar with third-party risk analysis.

Coming to a board meeting with these contextual pieces of information as a security leader will help both you and your executive team feel empowered to make informed decisions based on data you truly understand. When security leaders work crossfunctionally with the leadership teams at their organization, they are able to keep cybersecurity at the forefront of company decisions.

Advancing Your Business With Tactical Reasoning

It can be more effective to take it one step further and break down the report at a tactical level. Demonstrating risk associated with a vendor's security by the specific ways malicious activity could take place can give a more comprehensive and realistic picture of the path malicious actors can take. This is particularly important when it comes to getting board support for vendor changes or renegotiating business contracts. When you are looking for efficient approvals, showcasing the tactical steps taken to reach each decision in plain language will result in faster participation from the board and allow you to maintain a productive TPRM program.

Taking The Strategic Approach

The board will care about the strategic advantage vendors bring to your company as well, specifically if the vendor's cybersecurity posture will positively or negatively impact your vendor portfolio by partnering with them. Being able to communicate portfolio risk to the board and senior leadership can help justify decisions, such as when the security team wants to rethink vendor strategy. This is important in the current, changing environment where companies have to evolve their processes surrounding third-party risk in order to stay protected from malicious actors.

Successful communication with the board and leadership team is an area most departments struggle to master because of the disconnect between what the board wants to see, and the level of knowledge the board is believed to have on various topics. Presenting your third-party security program in a way that makes sense to the board, and also relates your goals to the overall company goals and operations will help you successfully demonstrate the need for the board to prioritize cybersecurity.

IN CONCLUSION

As the world continues to adjust to the "new normal", it's imperative that TPRM program managers find efficiencies wherever they can. Combining the steps above with the powerful tools found in BitSight for TPRM sets you on the pathway to creating a fully mature TPRM program that is fully scalable while being faster and less costly, and creates efficiencies that reduce risk and enable the business to operate more nimbly and more profitably.

To gain visibility into your third-party security footprint and start implementing security ratings into your vendor lifecycle, request a demo with the DVV Solutions team.

Go to https://www.dvvs.co.uk/contact

Call +44 (0) 161 476 8700 or email enquiries@dvvs.co.uk.

DVV solutions

About DVV Solutions

DVV Solutions are a specialist managed service provider of Cyber Security, Third Party Supplier Risk and Governance, Risk & Compliance (GRC) solutions. Our suite of consultative and managed services improve your ability to manage the myriad of enterprise risks associated with business process outsourcing and the cyber supply chain.

We have teamed with world-class thought leaders, industry bodies and technology providers to create best of breed TPRM services and solutions. For more information, please visit **www.dvvs.co.uk** or **Follow Us on LinkedIn**

BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Seven of the top 10 largest cyber insurers, 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit **www.BitSight.com**, read our blog or follow **@BitSight** on Twitter.