Unify Third-Party Risk and Cybersecurity for Sustainable Resiliency

ProcessUnity

INTRODUCTION

Organizations with unified risk programs are more efficient, more resilient, and onboard less risk than those with siloed third-party and cybersecurity teams.

By aligning their risk reduction efforts, procurement and cybersecurity can take the lead in mitigating two of the most significant risks faced by any organization: cyber and third-party.

While direct cyber attacks threaten to compromise sensitive data by exploiting vulnerabilities in an organization's controls, attacks on their third-party ecosystem may enable hackers to bypass internal controls, meaning even organizations with mature cybersecurity programs can have their data compromised and their reputations damaged. By aligning their efforts to protect sensitive data, procurement and cybersecurity can turn their shared risk into an opportunity to grow their function within the organization and become leaders in the effort to reduce vulnerability and increase resilience.

This white paper will begin with a survey of the risk landscape: first, it will outline the overlaps and dependencies that link cyber with third-party risk, the challenges that produce siloed risk programs, and the benefits of cross-functional collaboration for mitigating risk across both domains. Then, it will lay out the four steps to aligning cybersecurity and third-party risk management programs in your organization.

The next few pages will demonstrate the increased risk inherent to siloed programs, the business benefits of an integrated approach to third-party and cyber risk, and the feasibility of connecting these two functions within your organization.

By aligning their risk reduction efforts, procurement and cybersecurity can take the lead in mitigating two of the most significant risks faced by any organization: **cyber and third-party.**

CYBER RISK IN THIRD-PARTY RISK MANAGEMENT

Many procurement departments focus on limited, check-box compliance in third-party cyber risk, opting to assess must-have controls without embarking on the more rigorous evaluation that a cybersecurity program would demand.

Vendors and customers are onboarded with due diligence questionnaires that cover domains like compliance, physical security, financial risk, and identity management, but these assessments often overlook alignment with the organization's internal cybersecurity controls.

As more cyber-attacks originate in the vendor ecosystem, however, third-party risk managers are saddled with an increasing responsibility over their organization's risk posture. In 2021, Deloitte found that more than half of all organizations have been exposed to one or more third-party risk incidents since early 2020, signaling that third-party risk managers are often the first line of defense against hackers and cyber criminals. This shift has led to mounting pressure on third-party risk managers to emphasize the cyber domain and achieve greater visibility into their vendors' cybersecurity postures.

Gatekeepers and Guardians

Procurement departments face a challenge too great to be handled on their own: they must act as gatekeepers, ensuring that their organization doesn't onboard a risky vendor—but vendor risk means different things depending on an organization's internal priorities. For instance, an organization with known vulnerabilities in its own identity and access management controls would want to pay special attention to its third parties' information security and identity management policies to ensure it doesn't deepen its pre-existing weaknesses. A vendor with a moderate vulnerability in either of those areas may pose a serious risk to the above-described organization, meaning effective third-party risk management is only possible through collaboration with cybersecurity.

By aligning their risk management practices with cybersecurity, procurement departments can advance past reactive, check-box compliance to become risk leaders, catching risk before it's even onboarded. This means communicating with cybersecurity to learn the frameworks, standards, and controls already in place internally, then using that data to ask the right questions before a vendor gains access to your systems. By leveraging these insights, procurement can achieve a proactive risk posture and help guide their organization to a more mature information security program.

THIRD-PARTY RISK IN CYBERSECURITY

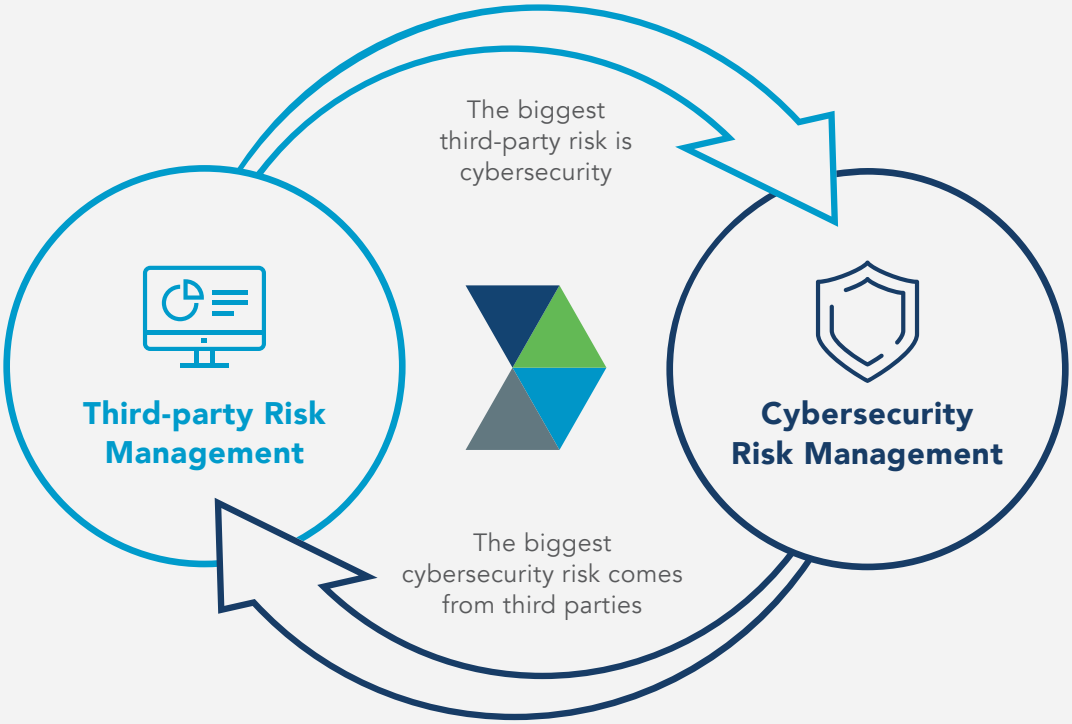
Cyber is one of many risk domains dealt with by procurement, but it is the primary focus of the cybersecurity team, meaning they tend to evaluate internal cyber controls with more scrutiny than procurement does their external controls.

This discrepancy can lead to hefty cybersecurity penalties against organizations with strong internal controls but weak external ones. In October 2020, Marriott was fined almost $24 million USD for GDPR non-compliance—not because any of its internal controls failed, but because a recently acquired third party had been compromised as far back as 2014. In cases like this, the checkbox compliance typical of many procurement departments' onboarding procedures isn't enough to prevent penalties or reputational damage.

Cybersecurity teams must be ready to own the consequences of data breaches and manage whatever incidents strike their organization.

Still, when over half of all cyberattacks originate in the third-party ecosystem instead of an organization's internal security architecture, this poses a problem: how can a team take responsibility for events that take place outside its purview?

To meet this threat head-on, cybersecurity and procurement teams must align their security practices and treat third parties as an extension of their internal framework. If this alignment provides procurement with an opportunity to grow their function, then it allows cybersecurity to achieve a new level of excellence in their domain: relating third-party and internal controls means not having to take the fall for a breach you couldn't see coming.



CHALLENGES TO ALIGNING CYBER/TPRM

Though cybersecurity and third-party risk are deeply interconnected, direct responsibility for these two domains is divided between different teams, meaning neither has complete visibility into the organization's risk.

This segmentation deprives each unit of the tools they need to complete their function: while the cybersecurity team lacks the leverage necessary to ensure responsible third-party risk practices, the procurement team lacks the expertise necessary to validate vendor controls.

Meanwhile, any disconnect between these teams results in myriad vulnerabilities for hackers to exploit—after all, the proliferation of third parties with wide-ranging data access and immature controls makes for an ideal target. By compromising one of these organizations, attackers can gain access to sensitive information without the ultimate victim's knowledge.

For instance, if an organization hires a public relations firm and allows them to create cloud accounts without consulting the cybersecurity team, then bad actors can use that firm as a backdoor into the organization's data without taking a risky direct stab at their internal controls.

Thus, to meet the rising threat of third-party cyber-attacks, Chief Information Security Officers (CISOs) and Chief Procurement Officers (CPOs) must foster cross-functional communication around their lowest common denominator. In other words, what controls do both teams currently evaluate? What objectives do they complete duplicative work for? By consolidating your efforts around pre-existing overlaps and identifying the remaining gaps, your organization can begin to break down siloes and treat your third parties as an extension of your security landscape.

Limited visibility between teams

Duplicate work

Security gaps in the third-party network

Lack of centralized control framework

STEPS TO ALIGNING CYBERSECURITY AND THIRD-PARTY RISK MANAGEMENTS

1.

ESTABLISH ENTERPRISE CONTROLS

Establishing enterprise controls means identifying the controls you perform today and the regulatory frameworks relevant to your industry, then using those standards to evaluate your practices. From there, you can begin compiling a list of controls you will need to implement and reducing redundancies by identifying overlaps between the frameworks you are using.

Your organization will not need to implement every control that's relevant to each framework you choose. Perhaps a security framework suggests controls regarding physical protections, but your organization doesn't use an office space—there's no reason to implement a control that doesn't apply to you. Similarly, there may be overlaps between the frameworks your organization uses. If you've chosen two different frameworks that both require the same password protections, then that overlap can be consolidated to a single password-related control. By identifying these overlaps and irrelevancies, your team can transform a cumbersome control burden into a manageable, cross-functional library.

Framework selection and control assignation tend to be conversations between the CISO and the board: once the CISO lays out the applicable standards and the board agrees on the appropriate level of granularity, then the cybersecurity team can begin developing controls and assigning owners. In organizations without a CISO or a cybersecurity function, framework selection is carried out by an external consultant. Either way, this phase begins with framework selection then moves into control consolidation.

2.

SCOPE QUESTIONNAIRES BASED ON RISK

Scoping questionnaires saves time for both your organization and your vendors: you might have three-hundred controls that you're interested in checking for, but depending on their service type, most of your third parties will only need to provide evidence for a fraction of what's in your framework depending on their service type. After all, vendor fatigue is a real concern in due diligence: it's much better to ask one hundred eighty questions and get a response in a month than to ask three hundred and chase responses for a year. By only asking the appropriate questions, your organization can achieve faster turnaround times and more thorough responses.

Mapping relevant questions to vendors means understanding who has access to which assets: a vendor with access to Protected Health Information (PHI) must be subject to more controls than the one who manages your janitorial staff. Similarly, it might be important to ensure that your janitorial staff is aware of your physical security controls, but that is likely a less important conversation to have with a fully remote PR firm.

By identifying the depth and forms of access granted to each vendor and scoping your assessments accordingly, you can get the right information when you need it, allowing you to make swifter decisions that support business operations. Additionally, a more focused pool of vendor responses enables procurement to take a more decisive approach to third-party risk management, allowing them to reduce cycle times and fulfill service or product requests faster.

Questionnaire scoping is typically carried out by procurement. If the team operates using spreadsheets and emails, responsibility for scoping will likely be delegated throughout the entire unit. Even smaller teams can, using an automated TPRM tool, maximize productivity by quickly scoping and distributing questionnaires.

3.

PUT ROBUST CONTINGENCY PLANS IN PLACE

Once you start receiving vendor assessments, you can begin comparing your internal cybersecurity controls with the ones your third parties have in place. When integrating cybersecurity and third-party risk management, it's best to treat your third parties as an extension of your organization—after all, their control effectiveness is now your control effectiveness. For instance, if your organization has password complexity controls in place, but grants multiple vendors data access without ensuring that their controls meet your maturity requirements, then the quality of your data security is, on average, reduced.

When relating internal to external controls, it's useful for cybersecurity to ask the kinds of access questions that procurement asked when scoping their assessments. If your organization has an internal control about user validation, then the next step is to ask procurement what kinds of user validation controls are in place in the vendor ecosystem. Each internal control should be matched by corresponding controls at the applicable vendors.

If integrating these two functions is about fostering communication, then this is the step where communication between cybersecurity and procurement becomes crucial. Procurement must share their questionnaire data with cybersecurity so they can map vendor responses to internal controls, and cybersecurity should eventually factor the vendor data into their overall control maturity ratings. It's only once your organization begins to evaluate these two domains in comparison to each other that you can be confident in your knowledge of which vulnerabilities are critical and where your controls provide strong coverage.

When integrating cybersecurity and third-party risk management, it's best to treat your third parties as an **extension of your organization**—after all, their control effectiveness is now your control effectiveness.

4.

EVALUATE CONTROL EFFECTIVENESS AND REMEDIATE GAPS

Once you've begun to review your assessments, you can start evaluating your vendors according to the applicable controls. Are they under-performing compared to you? Overperforming? If you find that a sizeable portion of your vendors are underperforming on a specific control, it may be useful to break down your vendor population by service type or geography, then develop an action plan to remediate that risk.

For example, maybe your organization has strong two-factor authentication controls in place to protect the system that stores your clients' PHI, but your vendor assessments reveal that one in five of your third parties has 2FA policies that don't meet your organization's maturity standards. This is where it can be helpful to start breaking your ecosystem down by geography and service type: maybe, when you sort your third parties by location, you see that all the vendors with insufficient 2FA controls are located in a specific country.

This might indicate that the regulatory environment in that region doesn't place the same emphasis on user validation, meaning you can either remediate this issue by paying special attention to third parties from this area—or, depending on your geographical focus, it may be more efficient to seek out third-parties from regions that require the protections you're looking for.

Control evaluation should be a conversation between internal and external control owners. Internal control owners should have access to a directory of external controls that are relevant to their domain, and they should keep track of the TPRM practices that impact their control. On the other hand, procurement should keep cybersecurity up-to-date on changes in the third-party ecosystem. It is only by consolidating information and maintaining cross-functional contact between control managers that the cracks between third parties and cybersecurity can begin to be filled.

CONCLUSION

The separation of cybersecurity and third-party risk is an illusion produced by organizational charts. The risks are powerfully interconnected, so your responses to them should be, too. By relating internal and external controls then evaluating them holistically, your organization can deliver the transparency needed to eliminate cyber vulnerabilities in your third-party ecosystem.

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States

NEXT STEPS

Request a demo to learn how ProcessUnity can unify your organization's third-party risk and cybersecurity risk management programs to achieve true risk resilience.

REQUEST A DEMO NOW

230301