onetrust

InfoSec's guide to Third-Party Risk Management

Key considerations and best practices

E-BOOK | MAY 2023

Industry experts

Jose Costa
Sr. Director, GRC Labs & Research
- OneTrust

Kevin Liu
Sr. Director, Information Security
- OneTrust

Tim Mullen
Chief Information Security Officer
- OneTrust

Zuzana Rebrova
Head of Third-Party Cyber Risk Management
- Swiss Re

Matthew Solomon
VP, Technology & Cyber Risk Management
- Humana

Ruo Xie
VP, Source to Pay
- OneTrust

Table of Contents

Third-Party Risk Management (TPRM) for InfoSec professionals

While working with third parties is essential to the success of almost every organization, it introduces numerous new security risks and challenges.

In the last year alone, 84% of security professionals experienced at least one significant disruption directly attributed to a third party. Another 66% incurred financial loss and 59% saw reputational damage from third-party incidents.[1]

Organizations across all industries are quickly — and painfully — seeing gaps in their current security programs. As the nature of third-party relationships continues to evolve, more external parties will have some level of access to your organization's internal data. Without a third-party risk management (TPRM) program, this evolution into an extended enterprise will only compound your risk exposure.

Unfortunately, most security professionals don't believe their organization has the in-house capabilities or resources to manage all the third-party risks they face.[2]

Our guide focuses on this exact challenge: How can InfoSec professionals build a TPRM program that effectively manages third-party risks?

We spoke with leading security experts across various operational functions, from CISOs to cyber risk managers to procurement leads, about their approach to working with third parties. Learn how to get buy-in from key stakeholders, the existing resources you can leverage, and how security teams can safeguard their organization's data as they scale.

[1] Gartner Survey Shows Third-Party Risk Management "Misses" Are Hurting Organizations

[2] KPMG's Third-Party Risk Management Outlook 2022

Approaching a TPRM program as an InfoSec professional

One of the biggest challenges in building a TPRM program is knowing where to begin. Whether you're starting from scratch or rebuilding an existing program, it's important to align with key stakeholders early to establish expectations and determine the scope of the program.

What are your key considerations when starting a TPRM program?

Jose Costa, Sr. Director, GRC Labs, OneTrust: I'd say the two most important things when starting a TPRM program are getting buy-in from the organization and understanding your business.

It's important to look at TPRM as an organization-wide exercise. The CISO can drive it, but management teams at the top have to be in agreement with what you want to do and how you're going to do it. TPRM programs require involvement from privacy, finance, legal, and other teams — is your organization ready to do this?

That brings us to the second part, which is understanding your business. Without that, you can't assess risk correctly. You'll negotiate with third parties very differently if you're B2B versus B2C, tech versus non-tech. It's not one-size-fits-all.

Matthew Solomon, VP, Technology and Cyber Risk Management, Humana: Get really clear alignment on the value you're trying to achieve. Do you want to reduce the number of vendor cybersecurity incidents over a period of time or better understand your vendor risk posture?

The more you coordinate and socialize your intended outcome with the leaders and stakeholders in the organization, the more you're able to set resource levels, measure whether you're actually achieving the value you want, and structure your program accordingly.

In addition to the usual stakeholders in a contracting process, the board of directors, risk committees, second- and third-line risk functions, and the leaders who are seeking the vendor's service are going to be critical in driving organizational change.

Zuzana Rebrova, Head of Third-Party Cyber Risk Management, Swiss Re: On the external side, I'd look at what's needed in the company's regulatory environment. And on the internal side, I'd talk to the CEO, executives, and compliance and risk managers to determine the company's risk appetite and relevant risk domains, whether it's cyber, privacy, financial, operational resilience, or some other specific risk.

Have a purpose in mind for your TPRM program, or create one together with the team, and make sure it aligns with your company's overall strategy.

> "Third parties are just another asset you're trying to manage. And with any asset, there's always a level of risk or a threat that comes with it."
>
> | Kevin Liu

Approaching a TPRM program as an InfoSec professional

Kevin Liu, Sr. Director, Information Security, OneTrust: You have to know:

- What type of services are they providing?
- What type of data do they have access to or are processing on your behalf?
- Are there any integrations between us?
- Are we going to embed them within our product?
- How critical are they to our organization?

Those are different ways to help identify third-party risks and understand their potential exposure and impact to the organization. Then, once you have those things, you can create an assessment process and assign a criticality to the third party.

Ruo Xie, VP, Source to Pay, OneTrust: When a security person is setting up a TPRM program, they mostly focus on the risk reviews and assessments. But third-party risk, to be truthful, is not just the risk of sharing data, buying software, or integrating various systems. Those are very important risks to be aware of, but there's also compliance and payment risks, the core financial health of the vendor — all of these other risks that are not just part of security.

In my opinion, TPRM is going in a direction where it's more of vendor management that manages the process, with support and stakeholders from different areas, like security, privacy, and compliance. The vendor management team (a.k.a., procurement) have visibility on all purchasing activity across a company therefore uniquely positioned to funnel vendors through the TPRM process.

Key takeaways:

- **Start with a clear understanding of your business.** The details of your TPRM program should be based on the maturity of your organization and its relevant risk domains.
- **Define the purpose of your TPRM program.** Align with executives and managers on your program objectives and how it contributes to the overall company strategy.
- **Establish TPRM as an organization-wide exercise.** Multiple teams are involved when it comes to third parties and it's critical to get their buy-in before the program begins.

> "Get visibility into the data and systems and understand where your data is stored. Third-party risk is not just about cyber or operational resilience — it's a complex process with a whole spectrum of third parties."
>
> | Zuzana Rebrova

Approaching a TPRM program as an InfoSec professional

How would you recommend an InfoSec professional start building their TPRM program?

Tim Mullen, Chief Information Security Officer, OneTrust: It depends on the maturity of your company. For example, are you a publicly traded company that needs to show an audit trail in a concise manner? Do you have specific audit requirements?

If I'm doing third-party risk management, I'm looking at vendors I'm purchasing from, partners I'm dealing with, if we're doing consulting work, and things like that.

For most companies, TPRM is not something new. But it's not perfect by any means either. A lot of companies start off with spreadsheets. They ask third parties for certifications and manually send questionnaires to get more information about associated risks.

Rebrova: I would start from the top. Management needs to understand that third-party risk really matters, what the impact could be, and how it could affect the company. Then identify the stakeholders or the core teams for the activity, such as compliance, procurement, and everyone who deals with third parties. In a smaller company, that may be specific subject matter experts. You also need to talk to legal teams about the contract process because a good way to mitigate third-party risk is to transfer it via the contract.

Liu: When it comes to assessing vendors, you should establish your requirements (e.g., security, ESG, financial), risk tolerance, and exposure posture up front. If a vendor is going to have access to sensitive data or integrate with your network or environment, what do you need to properly assess their security posture? If they don't meet your requirements, what's the next step?

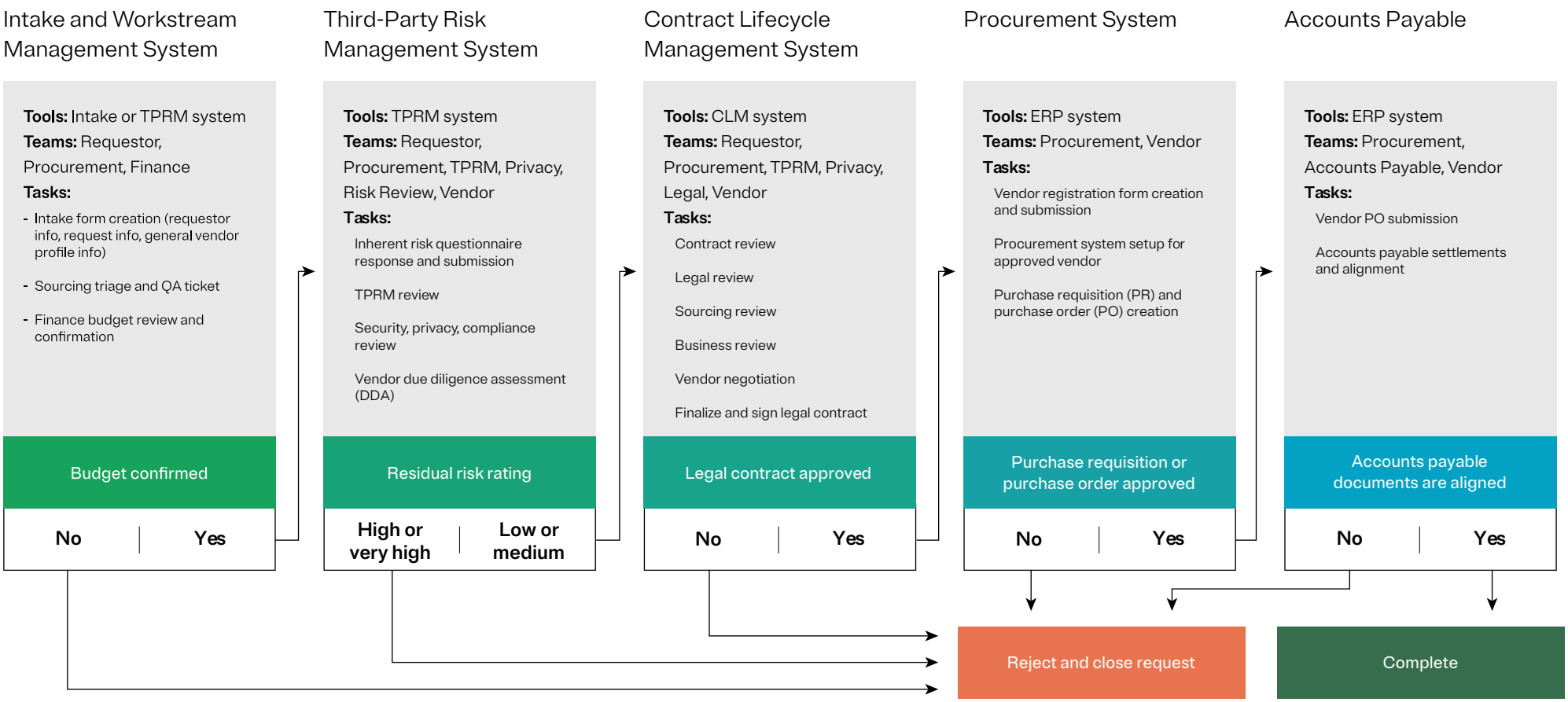
You have to be able to say, 'Inherently, I'm going to take on this much risk,' or 'Residually. I'm going to accept this much risk.' Residual is the preferred risk you're willing to accept, which means you have to do your due diligence and assess every service provider.

Even after a vendor is onboarded, you need to plan your monitoring process and workflow in case an issue comes up. Say something happens related to environmental, social, and governance (ESG) — who's handling that? It's not a security issue. If you define roles and responsibilities ahead of time, then you'll know the next steps. Plan the details of your program so you know exactly what the process is going to look like and also train your internal stakeholders.

Solomon: I'd say most companies already have some kind of a workflow for identifying a new vendor, bringing them into the contracting process, and ultimately onboarding them to provide a service. So typically, the cybersecurity team is trying to insert itself into the existing process far enough to the left to be able to drive decisions based on the results of your risk work.

Now actually making that happen could be done through a couple of different operating models. One operating model is the cyber team specializing in the expertise that's necessary. They create a clear risk picture of a given vendor, and then farm out the other contract-related steps that are necessary to create a complete program.

Approaching a TPRM program as an InfoSec professional



Approaching a TPRM program as an InfoSec professional

Another model is that the cyber team recruits the talent needed to do all those things, along with partnerships with the organization's procurement or other teams. I think both models work —which one you choose ultimately depends on what you're trying to solve for and how deep you want to go in managing vendor risk.

Xie: My team is called Source-to-Pay, and we handle strategic sourcing, third-party risk management, and procurement operations, including accounts payable and travel and expense.

I've been at companies where different teams, whether it's legal, privacy, or security, built a process that addressed all their needs and worked for them. But they didn't think about the experience of the user — the employee, the procurement team, or whoever has to participate in the process. That ends up with a very convoluted and confusing process people don't want to use.

It has to be easy for the end-user to understand. They have to want to use it. If you can achieve that, there's also the byproduct of it being very scalable. I want to dispel any confusion by consolidating all the vendor requests, putting out information about our process, and providing training and support channels.

Key takeaways:

- **Review your organization's existing TPRM process.** Take inventory of your current third parties and management process, then find the best way to insert information security into the workflow.
- **Identify the key stakeholders involved in the process.** Include anyone that deals with third parties, such as compliance, procurement, privacy, legal, and finance.
- **Consider the experience of all teams.** An effective TPRM process is one that makes it easy for the end-user to understand and use.

Approaching a TPRM program as an InfoSec professional

What does a typical TPRM process look like?

Xie: Our workflow is pretty standard for mature companies or companies trying to become more mature.

The overall procurement process starts by intaking vendor requests from employees. These requests usually include information about the employee and what service they want to outsource to a third party. You want to have a good intake system to ingest all vendor requests, triage information, and orchestrate work streams.

My team walks the request through a logical approval process, where we get budget confirmation first. Without that, we're not going to do everything else in the process.

Risk reviews are the most intense part of the process and take a lot of the security team's time. They can spend two to three weeks collecting information, reviewing SOC 2s, conducting penetration tests — all this can be a waste if there's no budget. You want your TPRM system to automate as much of the risk review and ongoing monitoring as possible, unless you're going to keep using spreadsheets and sending out questionnaires, which is hard to manage.

Once risk reviews and due diligence assessments have passed, then we go into contract review. Working with vendors pose business risks and legal risks, as well, and this is where we involve the legal team. A Contract Lifecycle Management (CLM) system will help automate the contract review process as well as manage renewals that are coming up, when contracts expire, when you can terminate a vendor, etc.

Finally, if the contract is approved, then we onboard the vendor into a procurement system, which is either integrated or part of an ERP system, and an accounts payable system to issue purchase orders and process invoices — then, you're off to the races.

Key takeaways:

- **Build a logical workflow aligned to your organization.** Map out each step, from intake to ongoing monitoring, so it fits the current systems and tools.
- **Get budget approval early in the process.** Before involving security teams, confirm the budget is approved for the outsourced service.
- **Allocate enough time for risk and contract reviews.** Risk reviews are often the most intensive part of the TPRM process and can take several weeks to collect information and perform testing.

Approaching a TPRM program as an InfoSec professional

What are the types of risks to prioritize when it comes to third parties?

Solomon: If you're in cybersecurity and there's already an existing process your team will integrate into, then you're probably directly focused on cybersecurity. If it's a larger initiative of the company, then you're probably thinking about resiliency risk, the financial health and reputation of the vendor, and cost factors.

I think it's very company specific — thinking about why you're launching a program in the first place, and what problem you're trying to solve each year.

Costa: Aside from the usual cybersecurity and privacy risks, there's also reputational risk. At the end of the day, you have to understand that even if it's a third party that does something wrong, it's your data. You're the one who's ultimately responsible and will be in the media answering questions.

Financial risk is another one. If you're not doing due diligence with vendors, you can get sued, you can be in breach of contractual agreements, laws, GDPR, and things like that.

There's also ethical risk, which may not be the CISO's main concern in the beginning, but is something to keep in mind. A venture capitalist or partner, for example, may require you to only do business with ethical companies. It seems simple, but it isn't. If you don't do a deeper investigation or ask the right questions, you don't know what you don't know.

And of course, there's the risk of breaching your customer's trust, which may be the most important one because it's very hard to fix. This isn't to fear-monger or scare the CEO or team. It happens everywhere, it's not only an IT thing.

Mullen: A lot of people don't understand that it's not only who you're doing business with, but it's who those businesses are doing business with — that's where the whole supply chain attack comes in.

You have to think all the way up and down the chain. You could have the 500 partners you do business with, but then they could have thousands on top of that they do business with. You can make it as broad as you want it to be.

It's all about building the maturity of your process, staffing, and how many resources you have. Obviously, there are a lot of considerations, but early on, you're trying to knock out the low-hanging fruit and figure out your risk exposure based on the partners you already have.

Key takeaways:

- **Consider risks beyond security and privacy.** When it comes to third parties, there are many other risks to keep in mind, including reputational risk, financial risks, and the risk of losing your customer's trust.
- **Look at the risk exposure of your entire supply chain.** Not only do you assume risks from your third parties, you also assume risks from their third parties as well.

Approaching a TPRM program as an InfoSec professional

Organization

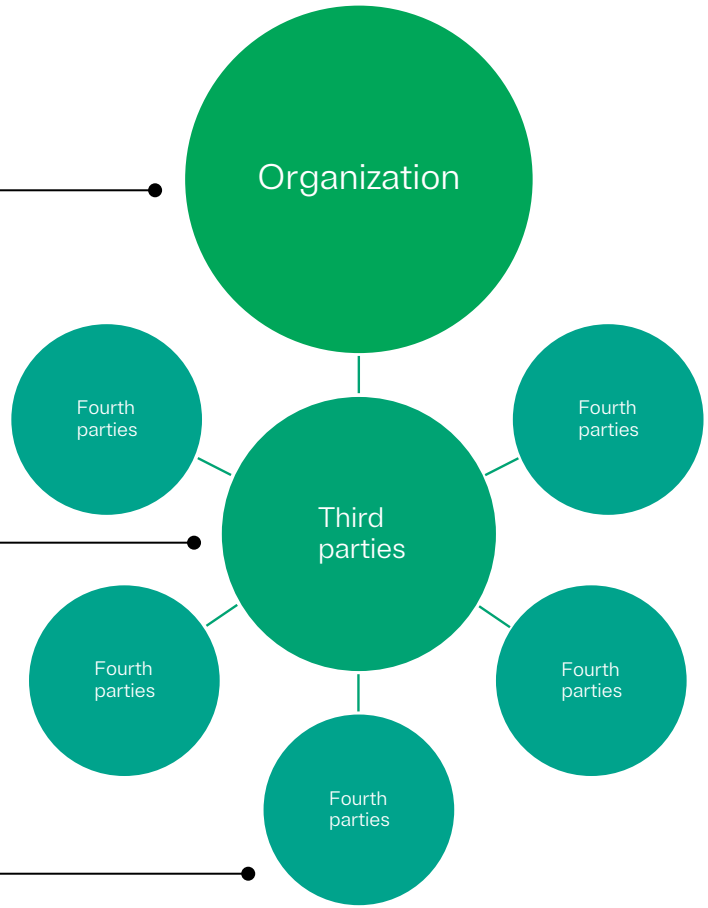
As organizations continue to prioritize growth and greater customer reach, third-party relationships are becoming more common across all industries.

Third parties

Third parties typically include partners, service providers, suppliers, and vendors. A recent survey reveals that organizations work with an average of 88 third parties, with larger enterprises (of 10,000 or more employees) using as many as 173 third parties.*

Fourth parties

Fourth parties are the third parties of an organization's third parties. While most organizations don't have direct contact with fourth parties, they can still impact your operations thanks to the interconnectedness of today's extended supply chain.



Source: Third-party risk: More third parties + limited supply-chain visibility = Big risks for organizations

Putting together the right resources and tools

Despite the complex and changing landscape in third-party management, you don't need a big investment to get a program off the ground. Most teams are already using tools that can be easily adapted for TPRM needs. Instead, most of the InfoSec experts we interviewed agree that building a dedicated team is more critical to a program's success.

Are there any InfoSec resources that can also be leveraged for TPRM?

Mullen: If you have a GRC platform, you could start there and build some of it yourself. Or if you have any of those third-party solutions tied into your risk management, it can give you scoring. There's Security Scorecard, BitSight, and other ones out there.

Are they perfect? No. But they give you a frame of reference right off the bat. They populate some of the data you need to kickstart your TPRM program and provide relevant information to start conversations with the vendors.

Another consideration is the return on investment from labor required to run the program. Can one person do this or do you need three people to do it? Can you lower your staffing costs with a centralized tool? A tool can help you assign resources, upload documents, and have one repository for everything. It makes processes and procedures a lot faster, easier, and more cost-effective. Then teams won't need as much formal training because they can leverage the guidance and checkboxes within the tool.

> "You don't necessarily need a solution, you just need to get involved in the process. As long as you have a way to get involved with procurement, sales, or whoever is bringing in new third parties, that's where TPRM teams can interject themselves."
>
> | Tim Mullen

Solomon: What I've commonly seen organizations do is either leverage their GRC tool or another existing tool that's already being used to integrate new vendors, often from a procurement perspective, and just insert themselves into that process. Perhaps the workflow triggers an alert to send assessment materials for the vendor to fill out before they advance to the next step in the process.

If your goal is to build the capability from scratch and don't have a ton of resources, you just have to onboard using what exists in the environment today. However, if your goal is to create really robust capabilities and a lot of the organization's procurement decisions hinge on the vendor's cyber risk rating, then you probably need new or add-on capabilities to your existing tools that can seamlessly gather the required vendor risk data, analyze it, and then report on results in a way that helps the ultimate decision-maker.

Putting together the right resources and tools

Xie: Whatever TPRM system a security professional ends up using, they could use it for intake as well. Intake is essentially a publicly available form for any employee to fill out so you can gather all vendor requests across the organization and properly triage and process them. So, if you only need it for security reviews, you can just tailor the form.

I'm using the intake form for everything — I want to know what we have to do from a financial perspective, from a risk review perspective, from a legal review or contract review perspective. For us, it's a one-stop-shop for all vendor needs.

From a systems perspective, you can look for the best-of-breed software, but it might not be the best fit for your system. You might have to do custom integrations or something along those lines, which is harder to maintain in the long run. It's important to think of the overall process or overall system stack.

Key takeaways:

- **Use existing tools to kickstart your program.** GRC or other risk management platforms can be used to provide the initial data for your TPRM program.
- **Don't assume best-of-breed software is always the right choice.** Instead, look at your existing tech stack and select software that integrates into the overall system.
- **Weigh your program's overall return on investment.** How much time and resources are dedicated to running your program? The right TPRM tool can increase efficiency, save costs, and make it easier to scale.

Does the TPRM process need a dedicated team?

Costa: You absolutely will need new resources for a TPRM program. It's a huge time suck. You're reviewing contracts and agreements, you're talking to legal, you're talking to privacy and InfoSec teams. You're negotiating with customers, going back and forth, assessing the responses they send you, incorporating internal controls.

Even with technology, it's going to take you time. But without technology, it's going to take you a ton of time.

Mullen: Yes, you usually do need a dedicated team. A lot of risk professionals have a Swiss Army Knife, broad range of security knowledge. Not super in-depth in any one area because they have to piece everything together, but they know enough to ask the right questions. A lot of them come from internal audit teams, Deloitte, KPMG, or a similar company, and have a strong breadth across many different disciplines.

Putting together the right resources and tools

Sometimes, you also need technical staff associated with TPRM. It's automated within our process that if there are certain questions — for example, about API keys or personal identifiable information (PII) data — it will involve a more formalized review that brings in our architecture team. So not only do you need risk-based individuals, sometimes you need technical individuals to have those more deep-dive conversations.

Solomon: There probably aren't too many cyber teams that have the excess capacity to lend to a really robust assessment process.

If your goal is just a light touch approach to get a general baseline of your risk environment, then that takes you down one resourcing path. You can start building partnerships with a procurement organization or other teams within the company that can allocate resources to help do the work. In any event, a level of partnership is necessary because no cybersecurity team can just insert contract language across the company totally on its own volition.

If your goal is deep engagement with your vendors to understand and remediate related risks, then your resourcing approach probably involves hiring people with contracting and negotiating skills to help develop an information security agreement. Probably someone with deep cybersecurity expertise who can look at vendor controls and draw useful conclusions about whether or not those are appropriate. And someone with a program management or communications background who has the ability to really affect the outcome of vendor relationships in a way that effectively manages risk.

Ultimately, resourcing success depends on your ability to package all that information into a presentation to get the right funding and be able to compete for the scarce talent that can do the work effectively.

Key takeaways:

- **Assemble a dedicated TPRM team.** Whether you allocate resources from existing teams or hire new individuals, TPRM programs typically require their own dedicated team.
- **Build a team with diverse skill sets.** Aside from information security expertise, a successful TPRM team requires professionals with contracting and negotiating skills, program management background, and communication experience.

Establishing TPRM's role within InfoSec

As third parties continue their involvement in an organization's day-to-day operations, they naturally become a bigger security priority. InfoSec teams are increasingly involved in the approval process of every third-party relationship, from initial contract reviews and due diligence to ongoing risk assessments.

What role does InfoSec play in the TPRM lifecycle?

Xie: Whenever an employee requests to outsource a service to a third party, we do an inherent risk review. If the review indicates that we need to conduct a full due diligence assessment on the vendor, then we'll have the different areas come in and review it as necessary.

For example, if it's a software vendor that we'll share data with through an integration, then security and privacy will be involved. If we're hiring a consultant that interacts with a government agency, then compliance is involved because there's a conflict of interest, bribery risks, and all that stuff. For our very risky vendors, all three of those teams might be involved.

Depending on the vendor, we ensure the right folks are included in the review and assessment process so we can mitigate as many risks as possible.

Mullen: We want to be notified of every new purchase, every new access point, or every new company or partner we're sharing data with because all of those could be risks.

All requests that go through the procurement process need security to sign-off. Think of it as gate one, gate two, gate three... security is one of the gates that you have to pass before the process will flow through and you'll be able to make a purchase.

Say, a request comes through to partner with a new company and give them all our PCI data... No, we're not, unless we have the right protections in place and the right understanding. We have a request for proposal (RFP) or a questionnaire that we send to vendors. Based on the responses, it might prompt us to have an actual phone conversation.

If they have certifications, like ISO certification, PCI DSS, SOC 2 Type 2, etc., it may be enough for us, depending on what type of data we're sharing with them.

We're going to have a lot more rigor when it comes to reviewing a security or financial services vendor versus a vendor that provides us with something like paper towels or toilet paper. But you can't buy anything at OneTrust without our team approving it. You just can't do it.

> "If you have a one-size-fits-all workflow, there tends to be a lot of confusion on what needs to be done, what doesn't need to be done. At some point, you will get your contract signed, but it may not have been reviewed in the right way."
>
> | Ruo Xie

Establishing TPRM's role within InfoSec

Solomon: In many company programs that I'm aware of, the vendor assurance activity really depends on being able to engage in the selection process early on and maybe even introduce some delays so you can perform the right due diligence, have the right conversation with the vendor, and remediate findings.

The business is going to push you to move faster than what might be appropriate. You're not going to have the right leverage with the vendor to get appropriate contract terms in place or get remediation actions taken as timely as you would like to.

You need to be early enough to perform a risk assessment in an amount of time that gives the decision-maker enough room to be able to make an informed decision based on the cybersecurity or risk posture. Being early also allows you to influence and insert information security agreement language into the contract because once the contract is signed, you're kind of between a rock and a hard place.

But you also need to be late enough in the process to really understand what the business use case is, what data is going to be involved, and what vendor connections need to be established.

1. **Intake third parties**
   - Centralize third parties in an actionable inventory
   - Prioritize inventory with inherent risk scoring
2. **Conduct due diligence**
   - Screen entities against compliance data sets
   - Review third party risk scores
3. **Assess third parties**
   - Automate risk assessments with collaborative workflows
   - Enable third parties to respond faster with AI autocomplete
4. **Review and mitigate risk**
   - Identify control gaps and review risks
   - Automate risk mitigation workflows and track progress
5. **Report and visualize**
   - Analyze key risk indicators and program metrics
   - Automate record keeping for compliance

Key takeaways

- **Involve security teams early in the vendor selection process.** Security and risk assessments help inform the stakeholder's decision and influence information security agreements with third parties.
- **Include the necessary teams and resources at each step.** Not every team needs to be involved at every step of the third-party process. Create a process that only brings in the appropriate resources when they're needed.
- **Tailor each risk assessment according to the vendor.** There's no one-size-fits-all approach when it comes to third-party management. Each risk assessment and review will depend on the vendor, the data that will be shared, and access to internal systems.

Establishing TPRM's role within InfoSec

What makes TPRM distinct from the broader InfoSec responsibilities?

Liu: If you look at the whole TPRM program, security is just one part. Other people are typically involved, including procurement, who helps get the best-of-breed and negotiates the price, your legal team, who reviews the contract and makes sure it has the right language to protect us, and the internal stakeholder, who identifies the service provider and owns the third-party relationship.

Security is involved to make sure third parties aren't presenting any additional risks in our environment that we're not aware of. And now, there's privacy involvement as well, depending on the data being shared or the vendor location, to make sure we comply with privacy regulations.

Mullen: A lot of the TPRM process deals with contract reviews, questionnaires, and performing due diligence on another company. It involves a lot of back and forth on the terms and conditions, and we get brought into that process a lot of the time, along with procurement and legal teams.

Costa: I do want to highlight that the contract review is super important in TPRM. You need to be best friends with your lawyers. When you're outsourcing, you also need to be clear on what the vendor is responsible for and what you're responsible for. And then incorporate everything into your contract and controls. A lot of TPRM programs fail because they just get the contract and review it according to a one-size-fits-all security standard.

Key takeaways:

- **Remember that security is just one part of TPRM programs.** Several other teams, namely procurement, legal, financial, and internal stakeholders, work alongside InfoSec throughout the TPRM process.
- **Check that all vendor responsibilities are included in the contract.** Contract reviews are a significant part of third-party management and should clearly outline the terms of the partnership.

Implementing a TPRM program across the organization

Even the best laid TPRM plan can be challenging to implement, especially across large global or distributed workforces. To facilitate your program roll-out, build relationships with all the stakeholders involved, look for all opportunities to automate manual steps, and provide adequate information and training to the entire organization.

How do you get your organization onboard with a new TPRM program?

Xie: We do roadshows, we have a distribution list for emails, and we have different support channels — a general channel, a procurement support channel, an accounts payable channel, etc.

My entire team is on the support channel and whether it's in their area or not, we all act as a helpdesk so people always feel like they're supported.

We also built a home page that guides people through the process, includes important links, and shares our procurement policies to give a little bit more coverage. For our high-use teams that work with vendors a lot, we provide training on how to go through the process, what to expect, and who to contact.

Solomon: I think the optimal model is where the information security team does a lot of research, builds relationships, understands the process, and then develops a clear proposal about what outcomes they want to achieve. Coordinate the proposal through leadership or maybe even to the board and say: 'Here's the risk we're trying to solve for. Here's the outcome we want to have related to that risk by the end of the year. Here are the resources we need to do it. And then, here are the business processes we need to affect as a part of that overall process.'

Or you could even start identifying the company's cyber risk issues today, and then go to the board next year and say, 'We've got X number of vendors, which is way too many vendors to be able to effectively manage this risk across on a consistent basis. We need to start reducing that overall vendor population.' That's not a cybersecurity-specific decision — that's a decision that impacts multiple parts of the company.

Ultimately, the point is to get involved with leaders as early as you can, depending on what your objectives are so you can influence the way the vendors are being managed holistically, not versus just performing cyber assessments that don't have the right level of impact.

Key takeaways:

- **Perform adequate research before proposing a TPRM plan.** Get an initial understanding on how third parties are managed in the organization and the benefits of a structured TPRM program.
- **Involve leadership as early as possible.** The success of a TPRM program relies on getting leadership's support from the beginning, and then communicating details of the program across teams.
- **Provide adequate education and training on the third-party process.** This can include knowledge bases, self-guided training, support channels, email distribution lists, and other documentation.

Implementing a TPRM program across the organization

What are the recommended protocols if TPRM teams notice an issue?

Liu: I make sure to assess and understand it first because not every single alert is equal. Go through the list of what you're monitoring for — the security posture, the social governance aspect, the financial health, and so on.

Say, your cyber monitoring tool shows a third party dropped from an A to a C and it should have a minimum of a B. If we identify that they're using an expired cipher for data protection or they have open ports that shouldn't be opened because of known vulnerabilities — well, those are pretty important to us. We'd set up a meeting with the product or security team to understand the reason behind the drop. If it's a critical issue, how long do we have to assess it and when do we need to make a decision? Even if it's a false positive, we still need to justify why it's a false positive.

Mullen: It depends on what service you're providing. In my previous experience in security for a healthcare company, we did a lot of business with hospitals, dental offices, etc. and they would get ransomware all the time. We just shut them off until they were all clear. We had about 50,000 customers and we just couldn't put anyone else at risk. Obviously, that's extreme.

With OneTrust, we could just turn off their single sign-on (SSO) until they're clear. Some companies want that also because they'd rather limit their exposure and only go to one area if they're having an issue.

Most of the time, it's a matter of reaching out to the third party for more information. But usually, it wouldn't reach us since we have lots of security controls in place to protect ourselves. That's part of the risk, right? You want to limit your risk as much as you can.

> "With every single vendor that we bring on, I always do a search and see if they've been breached in the last 12–18 months. It's a good way for us to understand and start having those discussions about their security posture."
>
> Kevin Liu

Key takeaways:

- **Create a step-by-step plan to assess security alerts.** Not all security alerts are equal. Have a process for assessing alerts and taking the necessary steps to address any issues.
- **Reach out to third parties for more information.** If your team notices a critical issue, contact the third party directly to investigate and limit any potential threats.

How to streamline the TPRM process

How do you streamline the overall TPRM process?

Xie: The big thing is automation. Without automation, you're kind of just redoing manual work in a system. It's a little bit better, but it's not a lot better — we want to be a lot better.

I look at the overall experience. What do employees experience when you go through this process? And what do we, from the security professional side, have to do to protect OneTrust? Finally, how much can we automate that so we achieve those two things with as few touch points as possible for the employee, and for security, privacy, and compliance teams?

If we can automate what's needed from a security or privacy posture perspective, we shouldn't need a human to review it. For example, if security says a vendor needs to have single sign-on (SSO) and the vendor can prove they have SSO, then the process should keep moving. The only time a human should be required to come in is if it deviates from the requirement or needs a business decision. Automation saves time and allows the security team to focus on the riskier, more complex vendor reviews.

Liu: It's always good to complete a threat model for every service provider you're using. Once you understand the service the third party provides, the data they have access to, and the integrations with our environment, start drawing out what a potential threat model would look like.

Each service provider is going to be different. The risk presented by a SaaS solution is going to be very different from software I purchase and deploy within my environment. But if you're able to create a threat model showing all the data going back and forth between your organization and the third party or even fourth party, you can better understand the risks and threats that are presented. Then, based on that risk, you can put together a remediation plan and assign a criticality level to the third party.

Maintaining security through a TPRM program

You can't set up a program once and then never look at it again. There are new cybersecurity risks and compliance requirements emerging all the time you need to be aware of, as well as different services or types of data your organization is starting to use. By making it a point to continually review and maintain your TPRM program, InfoSec teams can also discover ways to streamline the process.

How do you maintain a TPRM program?

Mullen: Depending on your company, you should revisit your TPRM program at least annually.

- Did a new contract come up?

- Did you start sharing different data?

- Did you start a different line of business?

- Did you do any mergers and acquisitions?

- Did you sell any companies?

All these questions determine if you need to pivot or make a change in your program. If you're doing the same business as you were last year and nothing's really changed, you might not need to do any active maintenance.

Of course, if there's something new in the market — a new vulnerability, new zero day, something that's piquing our interest — that can prompt a change.

Costa: Make sure you reevaluate and reassess any changes that have happened since the beginning of the contract. A common thing that happens is you sign on a vendor and then the scope changes.

For example, you could have implemented a new functionality and then all of a sudden, a vendor that was low risk now has access to highly sensitive data. Of course, there are data processing agreements (DPAs) to help address this, but even little changes in vendor relationships should go through another assessment process.

Key takeaways:

- **Review your TPRM program at least once a year.** Schedule time to assess your program on an annual basis or whenever there's a significant change to your company, the third party, or in the market.

- **Keep an eye out for changes in scope.** It's common for the initial contract scope to change after a vendor is onboarded. When this happens, have stakeholders reevaluate the existing terms and revise the contract, if necessary.

Maintaining security through a TPRM program

How are TPRM programs reported up to management?

Costa: Be careful with reporting because TPRM is one of those things that, if it works, it may not be something that you want to regularly report on.

If you're just starting to implement a TPRM program, you may report how many vendors have gone through the process, how many are compliant, etc. Or you may report the major risks you've assessed, how you mitigated them, and how you plan to evaluate them on a regular basis. It really depends on what management wants to see, but I would keep it high-level and at least make sure 100% of my vendors, irrespective of the size and complexity, go through the process and that the process is working.

Mullen: We don't have regular reporting. The team escalates to me when and if they need to. If not, it's their day-to-day responsibility. All the information is stored on our platform and we have holistic audit visibility over all of it. I can go in and look at all our different vendors, their rated risk, the last update, who approved it — it's at my fingertips if I want it.

Rebrova: Our management and stakeholders are definitely interested in reports and dashboards. We share a basic matrix on how many third parties we have, the distribution across low, medium, and critical tiers, how much risk exposure they introduce, etc. We also include how long it takes to assess a third party, the average remediation period, and any overdue risk mitigation activities. Another report is the third-party performance matrix. What is our service level objective, how cooperative or responsive is each third party, and other service level indicators.

Solomon: The information I've seen companies generally report to boards of directors or to senior leaders are the volumes of issues associated with vendors. Typically, if you're doing a vendor assessment, you're identifying certain risk-related issues and implementing a process to get vendors to address those issues. You want to report any high-risk issues that are past due or went past the service level agreement, which gives an indication of the current risk level.

Maintaining security through a TPRM program

Maybe you're really early in the game and just starting to introduce information sharing or information security into your contract. If that's a fundamental part of your program, you want to report metrics on your progress against that work, because contracts that don't have those terms are likely higher risk and you want your board to have that context.

If you want to see fewer incidents where your data is compromised when it's held by a vendor, then you want to report on the volume of vendor incidents over a certain period of time. Eventually, you'll reach a point of program maturity where you're able to report something more granular about overall vendor risk levels based on your assessment, or you're able to characterize your overall risk environment based on the number of vendors or the critical business process those vendors serve. Those data points paint the picture of what your overall risk level looks like.

The number of assessments and other similar metrics are helpful to me, as someone who's leading the team day-to-day because it lets me know how fast my team is working. But they're less directly related to the overall risk level. We could crank out a million assessments, but if they don't actually reduce our number of vendor incidents, then from a board perspective, the number of assessments doesn't really make any difference. What they want to know, I imagine, is the actual risk impact of your work and the actual risk level associated with your vendors.

If you have a tool that helps you be able to say this vendor is risk level X and you're able to aggregate that information across all your vendors, then you can quantify your overall vendor risk level. That's a really useful metric to bring forward and fewer companies I've seen have yet been able to get to that level of specificity.

Key takeaways:

- **Report on metrics appropriate to your program.** Depending on the maturity of your program, you may report on the total number of vendors assessed, overall vendor risk levels, or other relevant metrics.
- **Find ways to quantify your program results.** Management will want to know the actual risk impact of your work. Determine the best metric to quantify the overall vendor risk level and highlight that in your reports.

TPRM takeaways: Best practices and lessons learned

InfoSec professionals are already familiar with protecting against cyberthreats, complying with regulations, and safeguarding against ever-growing risks and breaches. However, as we've seen throughout this guide, TPRM programs span several other functions. Here are some key lessons our security teams have learned from setting up successful TPRM programs.

Advice for InfoSec professionals when building their TPRM programs

Costa: Ask questions. It's not the same to approve an application for the product team and to approve an application for the marketing team.

Who's going to use this vendor? What are they going to use the vendor for? How is the vendor integrating into our company? Why do we need the vendor's service? We often forget to ask why. You may not even need the new vendor because you have another application that does the same thing that has already been approved. Without knowing all these answers, you can't fully assess the vendor.

TPRM takeaways: Best practices and lessons learned

Rebrova: Start small with a minimal viable product, something that can improve the security posture right here, right now. There are established frameworks or certifications that can help and save time, so it's not really reinventing the wheel, but building on something that already exists. For example, we derived our questionnaire from the Standard Information Gathering (SIG) Questionnaire, a master questionnaire that we were able to leverage through the expertise of OneTrust professionals.

The tools and environment are evolving very fast. Until someone creates the perfect TPRM framework and implements it, your program is likely to end up becoming completely different. Start with a base that everyone can benefit from and build on because it's a never-ending process.

Solomon: An audit committee or board of directors will always want to see lower risk. The question then becomes how do you meaningfully quantify that out on a consistent basis? In information security, there are very rarely precise and actual estimates of real risk. So we have to look for indicators of risk, proxies for risk, or even more lagging indicators of the actual number of incidents. In terms of showing the actual impact of the program, the trick is really to get as close to the quantification of your risk level as you can and how you're driving that down.

Liu: Reassess your program, whether it's on an annual basis or more frequently, and continue to mature it. And don't just assess TPRM — assess everything that touches it. What's your policy related to vendor management? Are there any potential new risks identified by the organization's risk assessment team? Are there issues the organization identified related to this vendor or even another vendor in the same category? Bring in any relevant information and assess your TPRM program holistically to see how to move forward.

Key takeaways:

- **Start with a minimum viable program.** Draw from established frameworks or programs to improve your security posture in the quickest way possible.
- **Take a holistic view of your TPRM program.** Don't just review your TPRM program by itself — look at every team or function that touches it and how it impacts the entire organization.
- **Always ask why a new third-party service is necessary.** Oftentimes, companies already have an existing vendor that's already approved who can perform the required service.

Building Swiss Re's TPRM program

"In the summer of 2022, Swiss Re, a leading global provider of reinsurance and insurance solutions, decided to move its Third-Party Cyber Risk Management program completely in-house. Zuzana Rebrova, Swiss Re's Head of Third-Party Cyber Risk Management, explains how they transitioned from an externally managed program to rebuild their TPRM strategy and team from the ground up.

We actually rebuilt our TPRM program last summer. We had an external company develop our third-party cyber risk framework, which was a good start, but created a strong dependency — the process was removed from the things that were happening inside our company.

We didn't have the right tool for TPRM, so we sent out an RFP and had really clear criteria on what we wanted. First was the basic functional requirements and maintenance, as well as any unique functionalities that the tool provides. Then, the licensing model from a cost or financial perspective. Another big part was the potential synergy — considering what other teams can benefit from the tooling. We rated the tools according to these criteria and after we found our top three, we ran a proof of concept to prove each one's value.

We received 14 proposals but decided that OneTrust would be central to our TPRM program because we wanted a platform that procurement and other functions could use. I can say it was a bit selfish for us because we didn't want another tool that required extra steps to transfer data.

Our team is involved in the whole TPRM lifecycle, sometimes even in the RFP and selection process, but officially we're part of due diligence. Swiss Re has more than 10,000 third parties, but not all of them are cyber-relevant. Out of the total, I would say about 300-400 third parties are rated high or critical risk, whether from the cyber perspective, operational resilience, or financial perspective.

Right now, we have eight people on our team and our program's target objective is to make the process simpler and more agile. This focuses how we build our TPRM framework.

We use the 80/20 rule to minimize the effort required from our team as well as our third parties. For example, in our questionnaires to existing partners, we don't always have to ask what service they provide to our company or if they have a documented policy in place. Instead, we reduce the questions we already have the answers to and utilize self-reporting, external threat intelligence scores, or our own existing records to complete the third-party information. We only include the relevant questions, which saves us from starting from scratch every time and improves our partnerships."

How OneTrust helps build your TPRM program

OneTrust Third-Party Management enables greater risk visibility when managing third parties across the four critical trust domains: security, privacy, ethics, and ESG. The solution provides access to an array of functionalities, each built with automation and time-savings in mind.

Request a demo at www.onetrust.com.

onetrust

REQUEST A DEMO TODAY AT ONETRUST.COM

As society redefines risk and opportunity, OneTrust empowers tomorrow's leaders to succeed through trust and impact with the Trust Intelligence Platform. The market-defining Trust Intelligence Platform from OneTrust connects privacy, GRC, ethics, and ESG teams, data, and processes, so all companies can collaborate seamlessly and put trust at the center of their operations and culture by unlocking their value and potential to thrive by doing what's good for people and the planet.