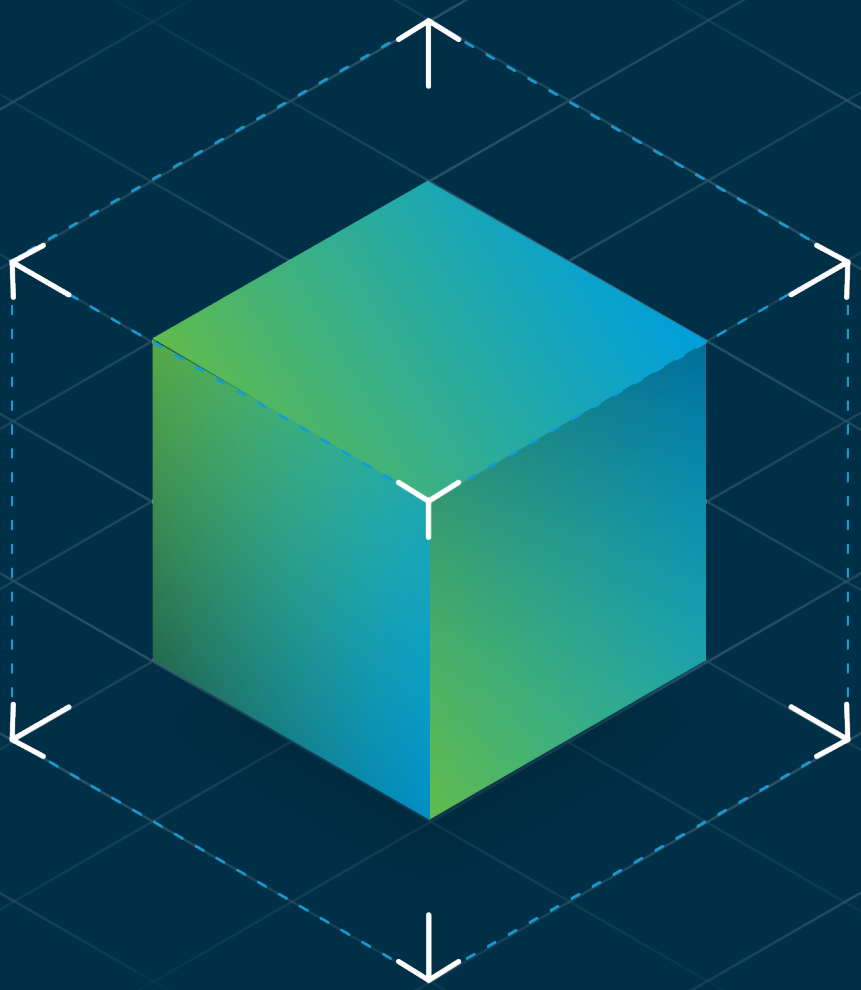
thirdpartytrust

5 Keys To Building a Scalable Third-Party Risk Management Program



Index

Introduction 2

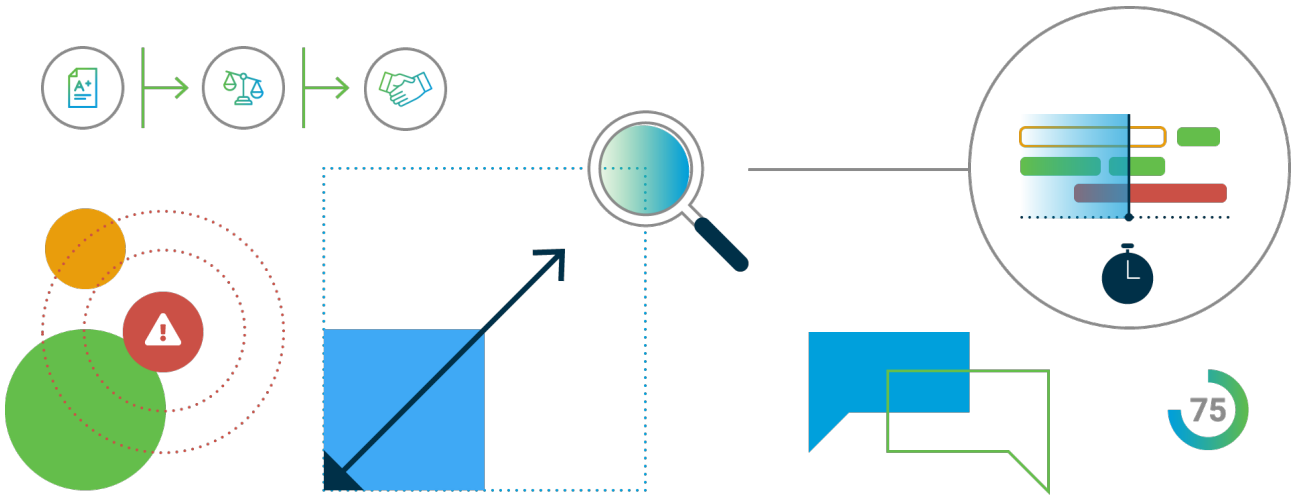
What Is a Scalable Third-Party Risk Management Program? 3

What are the benefits of having a Third-Party Risk Management program? 3

Five Keys to Building a Scalable Program 4

- **#1** Map your third-party inventory 4
- **#2** Identify Your Stakeholders And Get Them Onboard 5
- **#3** Perform continuous monitoring instead of point-in-time assessments 6
- **#4** Analyze and Score Results 7
- **#5** Address risk after having identified it 8

Conclusion 9



Introduction

Traditional security measures, such as SOC reports, on-site visits, pen tests and custom risk assessment questionnaires, are not scalable when assessing an enterprise's third-party ecosystem. They can be limited in scope, error prone, have limited reporting capabilities, and employ a one-size fits all approach, subjecting third-parties to the same set of questions. What's more, they require a lot of resources, which is likely to become an obstacle to scale.

It is now time to shift from one-off spreadsheets to a new approach which is less time-consuming and resource intensive for both enterprises and third-parties. It should cover for three critical capabilities:

- Program Management (from governance to training)
- Risk Assessment (from inherent risk to ongoing risk assessment)
- Monitoring & Response (from risk treatment to systematic monitoring)

What Is a Scalable Third-Party Risk Management Program?

A scalable program is one with continuous monitoring and mitigation of the risk that arises from third-party relationships. It has to be able to scale with business growth, which means having the ability to manage thousands of third-parties as effectively as you manage ten.

It's important to understand that all types of vendors, suppliers and providers are third-parties and therefore need to be properly assessed and managed.

The program is not meant to assess, but to assess **and** mitigate the risk associated with third-party outsourcing relationships. However, many programs assess risk and stop. They don't hold the third-party accountable for mitigation of the issues that were identified in the assessment, so they don't achieve the key goal of **continuous** risk mitigation.

What are the benefits of having a Third-Party Risk Management program?

- Consistency in rating the security posture of your third-parties
- Operational efficiencies, lower cost and defragment of the overall third-party risk management process
- Ensuring all of your third-party relationships adhere and comply with contractual commitments and regulatory requirements
- Access to data to make informed decisions on third-party relationships

Five Keys to Building a Scalable Program

#1 Map your third-party inventory

Start with the most important ones from a risk perspective. Those would be the companies that you exchange confidential and restricted information with, and the ones you grant access to your various platforms and infrastructure. Ask them who their third-parties are as well.

It will be useful to ask yourself these questions:

- What does "sensitive data" mean to your organization? Is it just personal identifying information, or are there classified programs or trade secrets at stake?
- Who do you share sensitive data with?
- Where does that data live? It could be stored in-house, in cloud servers or in third-parties' databases.
- Who is granted access to company data and infrastructure?
- Who develops software for your critical business applications and how mature is their software development process from a security perspective?

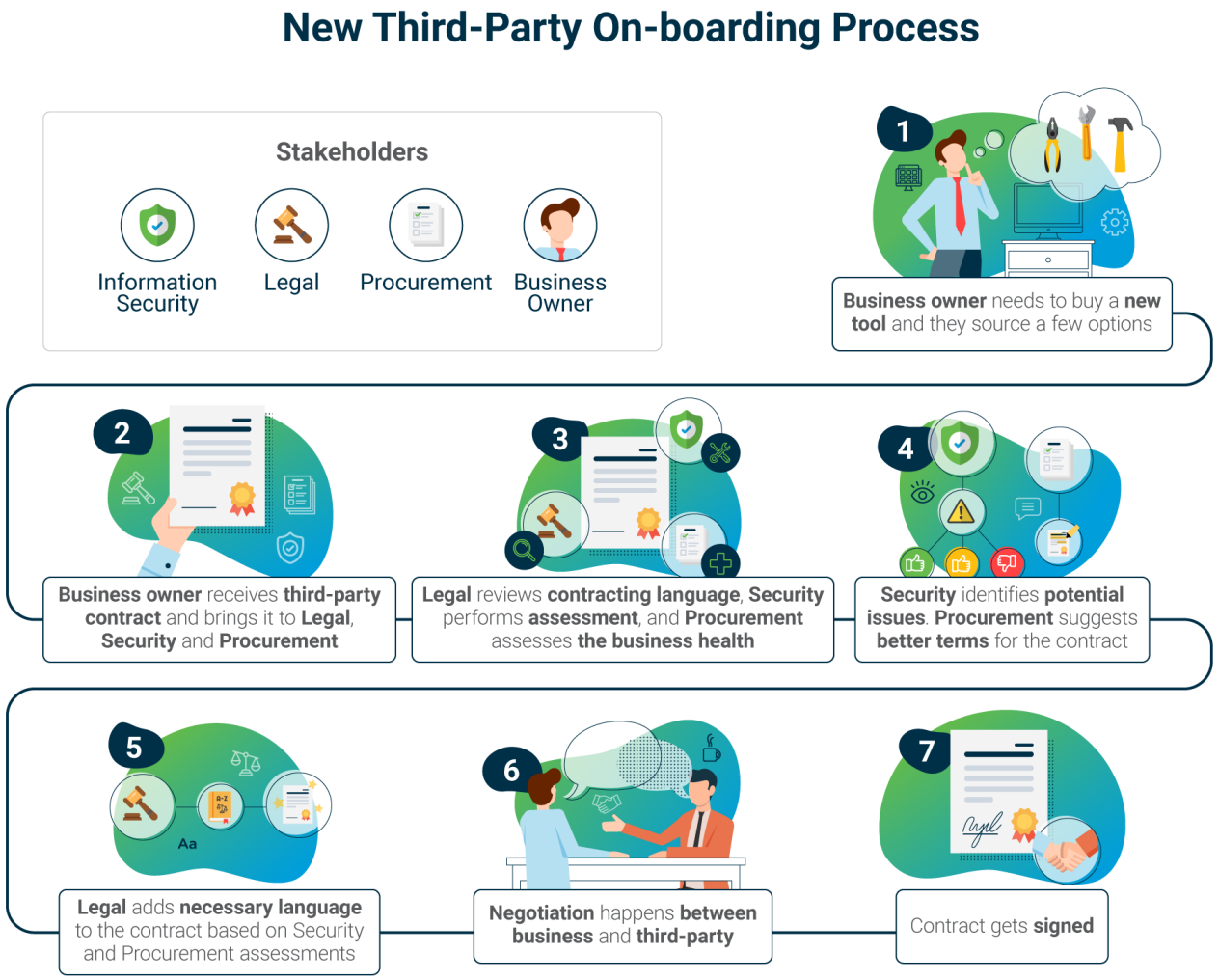
> ***PRO TIP:*** *New third-parties can be the starting point to build a scalable program. Once you have a mature framework, you can go on to address existing third-parties through your new process*

Get a list of any third-parties that are in the RFP process to serve your company, as well as a list of third-parties you currently engage with.

#2 Identify Your Stakeholders And Get Them Onboard

There are a handful of stakeholders around third-party risk management. The key is to have all of them working together with security from the beginning, instead of engaging a third-party without involving security teams at all or until the very end of the process.

This joint-effort model looks like this:



If the business owner or someone else from the company were to sign a contract before the security team has performed their review, they could be putting the company at risk.

#3 Perform continuous monitoring instead of point-in-time assessments

A scalable program should involve the ability to continuously monitor the controls that are in place at a third-party. This is much more effective than doing an annual assessment, which over time yields less insight and is static in nature, while expensive to perform.

How can you guarantee, from a security perspective, that you are OK for the remaining 364 days of the year?

> ***PRO TIP:*** *Technology is your key ally. Automation and real-time, continuous inputs from a reliable tool will contribute to the success or failure of each third-party and of the program itself.*

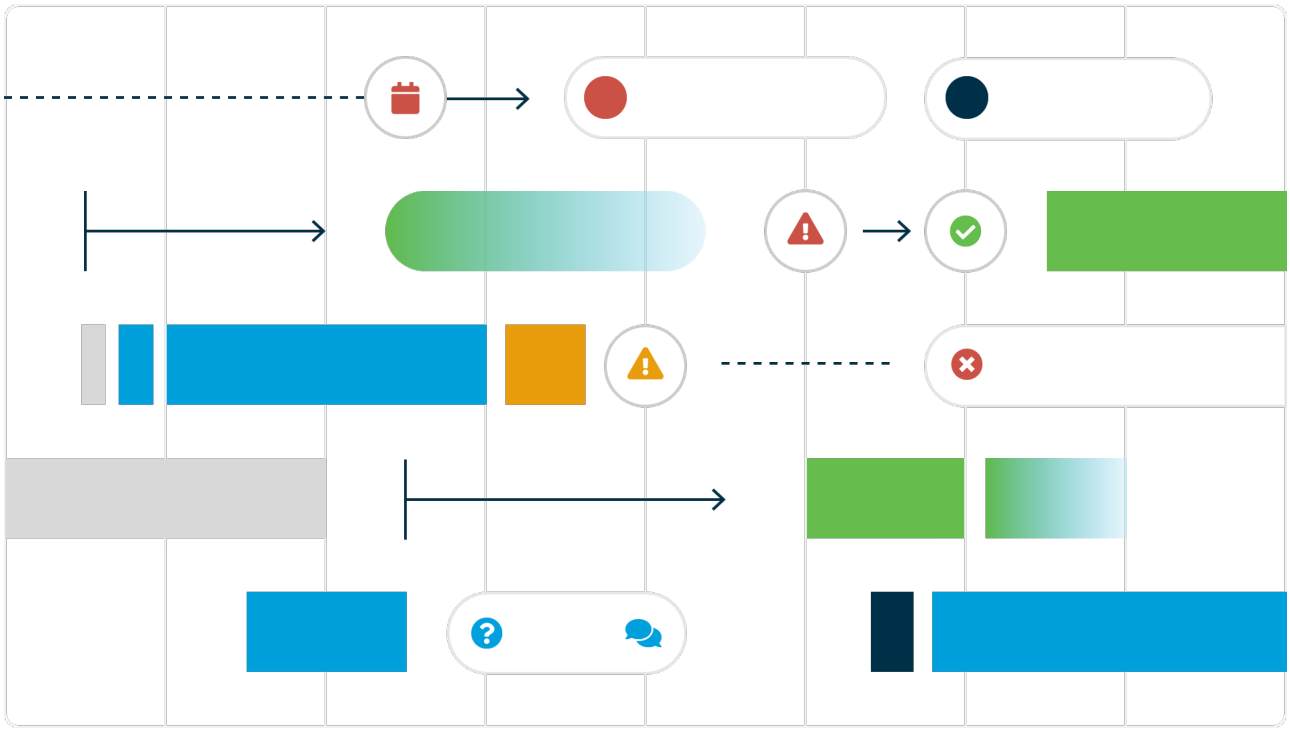
It might be helpful to ask:

- What are the new vulnerabilities that were discovered and need to be patched timely by the third-party?
- What are the changes in the third-party's network configuration that may result in an open threat actor to exploit?
- Has any new functionality added to a third-party service or product been properly tested and secured to ensure there are no vulnerabilities associated with it?

#4 Analyze and Score Results

Once you've completed and validated questionnaires, external assessments and/or certificates, you need to analyze and score all evidence so you can work on remediation. A consistent and easy to understand scoring system will improve decision-making, enhance visibility, and demonstrate the value of the program.

Objective measurement is important for monitoring third-party security performance across the organization. The scoring system can take many forms, but the important thing is that it will provide an understanding of how trustworthy a third-party is based on information provided by them and data gathered externally.



#5 Address risk after having identified it

The purpose of building a TPRM program is to mitigate risk, not to perform assessments. The process you build should not only provide you with findings, but also allow you to take action on those findings and mitigate them.

> *The purpose of building a TPRM program is to mitigate risk, not to perform assessments.*

When scaling this process, it will also allow you to discover unknown fourth-party or subcontractor relationships.

It's also important to consider that the third-party has to be accountable for the mitigation of any security issues that arise from this relationship. To that end, your contracts with onboarding third-parties should provide for three critical things:

- Right to audit, which gives you the ability to perform assessments
- Notification of any potential breach when it occurs
- Commitment to resolve security issues or gaps that are identified

Again, you need to have Legal, Procurement and Business Owners onboard to work towards the best possible contractual relationship in terms of security.

Conclusion

The management of third-party risk and security in general is a journey, not a destination. The key concept here is **“continuous”**: you need to monitor on an ongoing basis the controls in place and the changes in the relationship with your third-parties.

Apart from the obvious cyber and financial risks, there are other risk categories you need to think about: geo-political, macro-economic, social, legal, to name a few. A natural disaster, a political unrest or a global change in technology could affect the third-party relationship and suddenly disrupt your business operations.

The management of third-party risk and security in general is a journey, not a destination.

Therefore, this continuous monitoring cannot depend on point-in-time assessments. You need data inputs on a real-time basis in order to take the necessary precautions.

Don’t panic: Technology is here to help you scale your TPRM program to have a more accurate and timely understanding of the risk that exists within the third-party ecosystem. This means the ability to streamline not only the assessment process, but also complementary processes, like communicating with vendors and with company leadership.

thirdpartytrust

About **ThirdPartyTrust**

ThirdPartyTrust is a Chicago based SaaS company built on the premise that third-party risk must be managed in a simple and scalable way. Our network-based approach allows companies to streamline the information gathering and communication process while conducting security assessments. At the same time, third-parties are able to maintain security data in one central location and share it with their customers.

To learn more about our third-party risk management platform, request a free trial.