Vanta

From reactive to proactive:

How to minimize third-party risk with strong vendor management

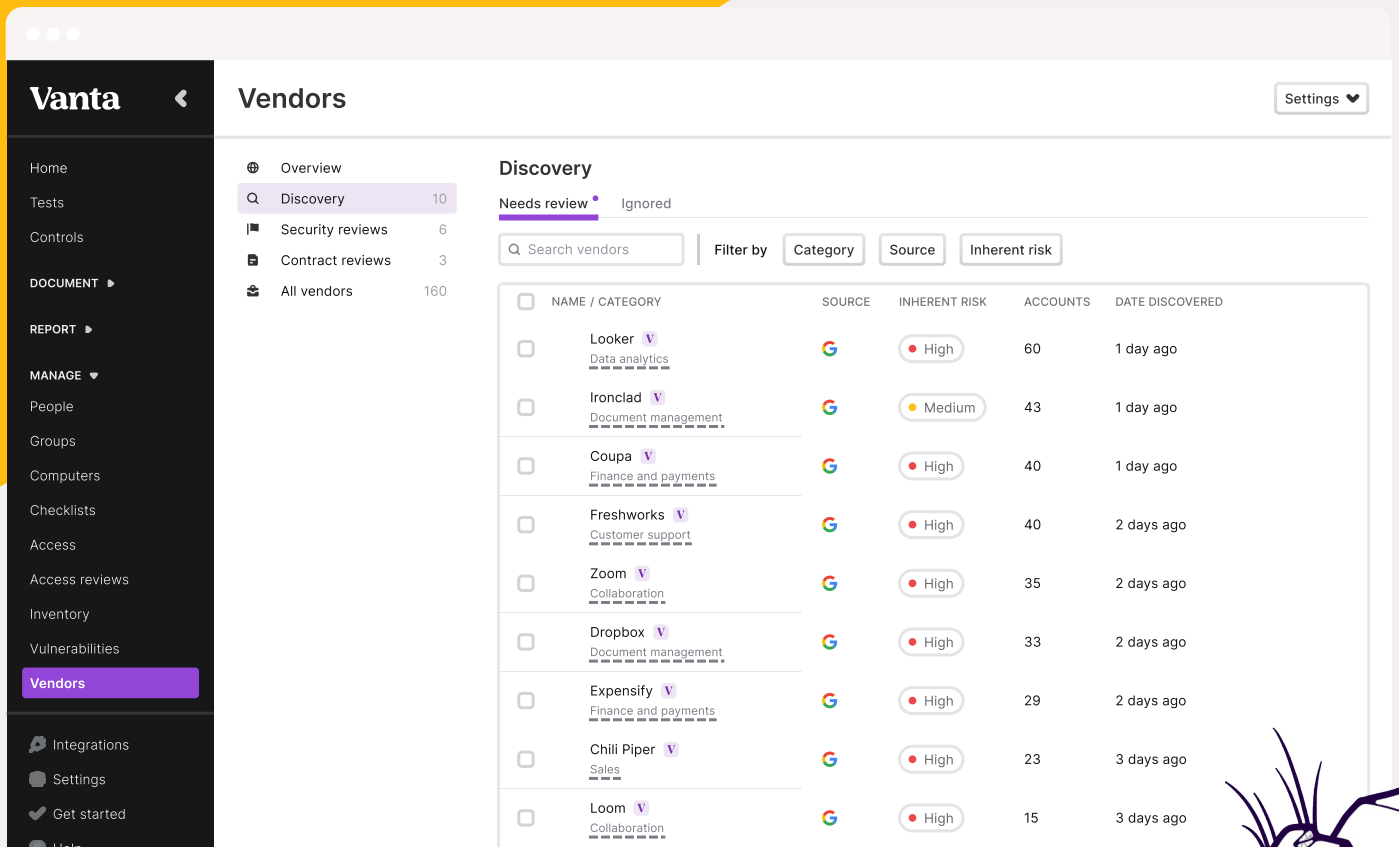


Table of contents

03 Introduction

04 The challenges of managing vendor risk

- 05 Limited resources mean limited visibility
- 06 Too much manual work
- 06 Maintaining strong security while enabling the business

07 Best practices for building & implementing a vendor management program

- 08 Inventory vendors — and follow the data
- 08 Prioritize vendors by risk and criticality
- 09 Perform security reviews
- 09 Establish a cadence for re-assessments
- 10 Conduct regular access reviews
- 10 Set the right expectations

12 Streamlining & automating vendor management with Vanta

14 Special thanks to our expert contributors

Introduction

Having a vendor management program in place isn't just required by compliance frameworks like SOC 2 and ISO 27001. It's also a critical part of a holistic trust management strategy.

With the proliferation of SaaS tools, however, implementing a vendor management program has become more complex and challenging. Employees today are increasingly bringing new tools into an organization before their security and IT teams have had a chance to thoroughly review them — increasing the attack surface and giving bad actors additional avenues to access sensitive business data.

The typical organization, for instance, uses an average of 110 SaaS apps spanning productivity, collaboration, design, analytics, finance, developer tooling, administrative software, and more. And with 60% of data breaches happening via third parties and companies taking an average of 280 days to discover a third-party breach, overstretched security teams need a strong program for managing vendor risk to stay compliant and secure — and deepen trust with their customers and partners.

This guide brings together perspectives from the frontlines of vendor security management. You'll also learn how security teams can enable the business to move quickly instead of being inadvertent gatekeepers.

What you'll learn:

Insights and best practices from tenured security and compliance leaders on how to manage third-party vendor risk while dealing with unavoidable challenges like limited resources and repetitive manual processes.

The challenges of managing vendor risk

As a requirement of compliance frameworks like SOC 2 and ISO 27001, vendor management programs typically involve performing an initial security risk assessment when a new vendor is being considered, establishing a regular cadence of security reviews for existing vendors, and quickly remediating issues if and when they arise. As of 2022, SOC 2 specifies at least seven controls that can only be satisfied by a vendor management program.

In addition to being a compliance requirement, having a comprehensive vendor management program with well-defined processes is a security best practice — and key to establishing and deepening customer trust.

As Gig Walsh, Director of Security & Compliance at LinkSquares, puts it, "I realized from my years of [working in] security that when we put data in someone else's cloud, if they have a breach, it's still my fault, right? I own the data, and it's my job to do that due diligence."

While it's clear that vendor management is important, implementing a robust program is far from straightforward. Compliance frameworks don't provide specific recommendations, leaving security teams to figure out how to meet requirements on their own so they can successfully pass an audit. They also run into additional hurdles that make it harder to manage vendor risk.

> "The most important thing to us is maintaining customer trust."
>
> **Gig Walsh**
> Director, Security & Compliance
> LinkSquares

Limited resources mean limited visibility

In the current economic environment, security professionals are finding themselves doing more with less, no matter where their organization is on the security journey. Solo practitioners and small teams facing tighter resources are finding it especially difficult to run a comprehensive vendor management program.

"If you're looking at a maturity model," says Aaron Kraus, Director of InfoSec at ButterflyMX, "level zero [means] everything is ad hoc and everything is chaotic."

In order to get visibility and control over the vendors being brought into their organization, security teams with limited resources end up spending too much time asking each department what tools they're using and using spreadsheets to keep track of everything. The lack of visibility is further exacerbated by shadow IT, as employees bring on vendors without the security team's knowledge or approval.

Too much manual work

Many resource-constrained security teams are also bogged down by manual processes, whether it's performing vendor risk assessments, chasing down vendors to fill out security questionnaires and provide their security certifications, or conducting ongoing security reviews.

Manual processes like these hamper efficiency. More often than not, critical vendor information is scattered across multiple tools, requiring manual consolidation of notes and findings on individual vendors and making it difficult to get a holistic view of vendor risk.

As the first, and only, security hire at ButterflyMX, Aaron Kraus is responsible for building both the internal and external-facing security programs at the property access management company. When it comes to annual security reviews, he's a "one-man shop of actually doing all the work — scheduling it, coordinating it, reporting the result."

Automating manual work would be especially helpful in two areas for Aaron: streamlining document reviews for low-risk vendors like major cloud service providers and setting reminders for infrequent, recurring tasks like annual reviews. "If a platform can automate that for me, it frees me up to work on trickier stuff," Aaron says.

Maintaining strong security while enabling the business

Managing vendor risk can also be a balancing act. On the one hand, security professionals want to be a strong partner to the business and enable teams within their organizations to find and use the best tools available. On the other, they're responsible for staying compliant and maintaining a strong security posture.

Acting as a gatekeeper to new vendors and implementing lengthy and complex procurement processes can have the unintended effect of leading employees to more shadow IT. "Being a security guy who always says no doesn't work," says Gig Walsh. "You have to say, great, let's figure out a way where we can make this work and lower risk."

> "We don't say yes or no to the business. We just make a recommendation based on risk."
>
> **Gig Walsh**
> Director, Security & Compliance
> LinkSquares

Best practices for building & implementing a vendor management program

Managing vendor risk with limited resources, limited visibility, and mountains of manual work is undoubtedly challenging. There are, however, a few key steps to setting up a vendor management program that can help you streamline and prioritize your efforts.

01 Inventory vendors — and follow the data

You can't fix what you can't see, so the first step to operationalizing vendor risk management is to do an inventory. Creating and maintaining a comprehensive list of all the vendors used by your organization gives you a starting point for determining where there's potential vendor risk and helps you ensure that all vendors are subject to the same security and compliance standards.

Sean Jackson, Director of Trust at Spiff, Inc. also recommends doing a data mapping. "Talk to the heads of every department and say, tell me all the tools you use," says Sean. "What data do we get from them? What data do we give to them? Where does it come from? Where does it go? What is it used for?"

Aaron implements a similar model of "follow the data" at ButterflyMX. "When thinking about third-party risk management, it's tough to get your arms around securing a single organization, much less expanding that reach to uncover all links in your supply chain," he explains.

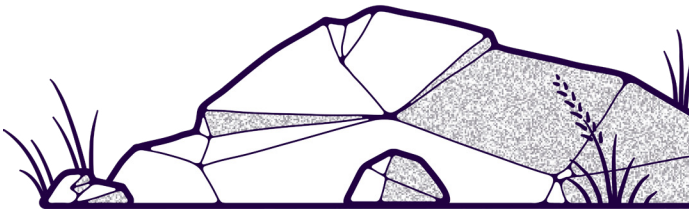
"Figuring out where your data is going, whether that's third-party regulated data like PII or company confidential data or intellectual property, is a critical input to building a third-party risk management program," Aaron says. "If you're not aware of where your data is being shared, analyzing vendors who may or may not be touching it is not going to provide a whole lot of value. So make sure you've got your vendor inventory as well as your data set inventory and data flow diagrammed out."

02 Prioritize vendors by risk and criticality

Once you have an inventory, the next step is to prioritize your vendors based on risk and criticality. In other words, which vendors have access to sensitive data or systems? And which vendors are critical to business operations?

Using a risk rubric ensures that you apply standard criteria when assessing vendor risk. Categorizing vendors into high, medium, or low risk also helps you surface the vendors that need additional attention.

"We've got some mission-critical systems that don't have any PII. If those get deprioritized in an annual review and we review them in an 18-month cadence from a security risk standpoint, I'd be comfortable with that," says Aaron. "Making sure that I've categorized those systems and figure out which ones are truly high priority and which ones are going to materially impact my security—those are the ones that with limited resources I'm going to prioritize."



03 Perform security reviews

While vendor security reviews can be time-consuming, there are a few ways to streamline the process, particularly if you have limited resources. Aaron, at a minimum, looks for a SOC 2 Type II report when performing security reviews for SaaS providers.

"I'm specifically looking at two things if it's very, very time constrained," Aaron explains. "Number one, I review the scope in great detail to make sure that the services that we're actually going to be using are part of it. Step two is analyzing the findings to make sure that what the auditors looked at, obviously whatever was in scope, [had] no deficiencies or issues noted with the controls."

If there are no findings, then "things are pretty easy," says Aaron. "If there are findings, then you have to do a little bit more analysis and figure out if this is a material weakness that could impact my use of the service."

For Sean, it's important to keep in mind that "no one has 100% security." If a vendor's SOC 2 report has a finding, have a discussion about it to understand how quickly the vendor fixes vulnerabilities and how they prioritize fixes.

"If you are focused on your criticals and your highs and you leave your mediums, then I don't trust your security program to be more than a checkbox," Sean says. "If you're fixing the criticals and the highs, you are worried about the check box. If you're fixing your mediums, you're worrying about the real-world activity."

This level of detail about a vendor's day-to-day security practices provides an additional layer of input in your assessment. "All the context around a vendor makes it so I know what I'm dealing with," explains Sean. "That's because the hardest thing you're trying to cut through is ignorance of a third party. You can't see what they're doing. You aren't a fly on the wall and don't have access to their tickets. You don't know how they deal with security. All these things go into what my posture should be."

04 Establish a cadence for re-assessments

In addition to going through an initial security review, each vendor in your organization also needs to be re-assessed on a regular basis. The cadence can vary depending on the risk level they're assigned and other factors.

For example, Aaron typically does an annual review at ButterflyMX for critical vendors that touch sensitive data. He recommends asking the following questions when re-assessing vendors: "Have we had any data breaches with this vendor in the past and have we seen any variance? Do they have no findings one year and then a bunch of findings another year? I would consider them a higher risk based on that and therefore subject to more in-depth scrutiny at the next reassessment," explains Aaron.

At Spiff, Sean reviews sub-processors every six months and other vendors annually. He also sets up alerts with a privacy tool that notifies him when there's a breach. "If someone has a leak or breach and it doesn't affect us, then I just want to know what's happening," Sean says. "If someone has a breach, and it does affect us, I'm looking for a phone call. If I don't get that phone call, I know they're not adhering to their agreements."

05 Conduct regular access reviews

Performing periodic user access reviews to verify, identify, and validate access rights and privileges is another compliance and security control mechanism for mitigating vendor risk.

At LinkSquares, Gig performs quarterly access reviews for systems that are within scope for SOC by setting up a 30-minute call with the appropriate team member. "We do it via Zoom, and we're logging in, looking at accounts, getting an export at the time, and then offboarding or changing permissions as necessary. And I document every one of those with a ticket if I take action."

Conducting synchronous access reviews also gives Gig the opportunity to reinforce security best practices. As he explains, "It's nice to actually have that review with the team quarterly to keep in touch and say, 'Wow, you know you're the owner [of this tool], and you've got 12 administrators. Maybe you don't need to make everybody an administrator. Let's give these people other permissions. It's a nice way to keep them honest."

06 Set the right expectations

An important part of managing vendor risk is to set clear expectations within your organization around working with third-party vendors.

"When the business needs something, I would hope that they haven't just picked a product," Gig says. "They would go through an RFP process to look at the top three vendors, and that's when security starts. Right before we even have the relationship, we should do a vendor risk assessment."

Defining and socializing vendor risk policies can help guide the selection process and establish criteria for when the security team needs to be looped in — helping to ensure that this happens before a new tool or vendor is brought onboard.

A set of well-defined policies can also include baseline requirements for vetting third-party vendors to streamline the process. "It removes me as a single point of failure," explains Aaron. "If you're bringing on a new vendor and they're not touching sensitive data, they have some security boxes checked, and they can provide a SOC 2 Type II or an ISO certification, then I like to remove myself from the process altogether but make sure somebody at the company has reviewed those things." For vendors that touch sensitive data in any way or can't provide the minimum level of assurances, that's when Aaron wants to get involved.

Successfully implementing a vendor management program ultimately requires aligning your security practices to your company culture. "The most important thing is figuring out how your organization actually works," Aaron says.

ButterflyMX has a decentralized culture, so Aaron has built his programs accordingly. "Stewards of different systems are responsible for performing certain actions, like doing their annual access reviews based on input that I provide them," he says. "Culturally, and the way that teams work here, that makes more sense. It's easier than trying to have one or two people with all the knowledge that's needed. And more importantly, just the way that we're geographically distributed, having people outside of time zones doesn't support the way that the business needs to work."

“Security should always be aligned to business objectives. It does actually have real-world impacts.”

Aaron Kraus
Director of InfoSec,
ButterflyMX

Streamlining & automating vendor management with Vanta

While managing and reviewing vendors can be a tedious and time-consuming process — particularly when you're working with dozens or hundreds of vendors — it doesn't have to be.

Vanta's Vendor Risk Management solution helps security teams streamline, automate, and scale the vendor security review process, reducing the time it takes to find, score, review and report on vendors by over 90%. Vendor Risk Management enables:

Automatic vendor discovery: Vendor Risk Management automatically surfaces applications that are connected to your organization's IDP or workspace using system integrations so you can quickly and easily create a thorough inventory of vendors. You can also upload your own vendor lists to create a single source of truth.

Increased visibility into shadow IT: Most security teams have no way of knowing when an employee starts using a new tool. Vendor Risk Management changes that with automatic vendor discovery and enables notifications when new applications are brought into your organization.

Standardized vendor risk assessment criteria: Vendor Risk Management comes with a built-in risk rubric that calculates the risk of a vendor (low, medium, or high) based on their access to sensitive data, business criticality, and other factors. The rubric can be customized to your organization's specific criteria so you can assess vendor risk consistently.

Fast & efficient security reviews: For high-risk vendors requiring a security review, Vendor Risk Management provides a centralized hub for gathering vendor security documents, noting your findings, and creating follow-up tasks. And since security reviews need to be repeated on regular cadence, Vendor Risk Management lets you set up reminders.

Easier collaboration with stakeholders: When it comes to onboarding new vendors, security teams often work with many stakeholders, including the department requesting the vendor as well as legal and finance for due diligence. Vendor Risk Management provides a single hub for cross-functional coordination.

Integrated compliance & risk management processes: While vendor security is typically siloed and disconnected from other programs, Vendor Risk Management is integrated into Vanta's Trust Management Platform. This lets you map your vendor security review processes to relevant controls, making it easier to demonstrate compliance to auditors and other stakeholders.

More control over user access: Vendor Risk Management works seamlessly with Vanta's Access Reviews to simplify and accelerate user access review. Quickly review, adjust, and report on user access via system integrations, simple reviewer workflows, and remediation management capabilities.

With Vanta's Vendor Risk Management, you can exceed and demonstrate your security commitments, no matter the size of your team. By streamlining and automating your vendor management workflows, Vanta helps minimize manual work, maintain a strong security posture, and focus your efforts on strategic security initiatives that move your organization forward.

Special thanks to our expert contributors

We'd like to thank the following security and compliance leaders at Vanta customers ButterflyMX, LinkSquares, and Spiff for taking the time to share their expertise with us.

Sean Jackson, Director of Trust at Spiff, Inc.

Sean has been in Information Security for over 12 years, with experience in almost every niche of the vast landscape InfoSec offers. He has built security programs from the ground up for startups and has been one of the hundreds on the security team at a Fortune 100 organization. He has helped organize regional conferences and has spoken many times at them and can be found on YouTube trying to help others get started in their careers. He is a husband, father, fur dad, and adoptee. He plays on the neurodivergent team and recognizes (some) of his privilege and tries to support minorities to make up some of the difference.

Aaron Kraus, Director of InfoSec at ButterflyMX

Aaron combines a professional background of InfoSec risk management with writing and teaching skills spanning 20 years across government, financial services, and tech startups. This includes designing, implementing, and running the worldwide onsite Third Party Risk Management audit function for a major US bank, comprising the creation of a control framework, audit procedures, and operation of the global audit team. Aaron uses his experience to build security cultures that not only make security everybody's responsibility, but also equip them with the skills and knowledge needed to be cyber defenders every single day.

Gig Walsh, Director of Security and Compliance at LinkSquares

Gig Walsh is an experienced information security executive highly proficient in implementing effective strategies and programs. He provides direct guidance and oversight to GRC projects, offering practical solutions for complex risk and compliance challenges. His expertise lies in aligning security activities with business objectives, streamlining processes, managing risks, and optimizing resource efficiencies. A skilled leader in building and managing successful cybersecurity teams, he prioritizes collaboration, trust-building, and empowering his direct reports to achieve strategic goals and be the best they can be. He lives in NH with his family and dogs. In his spare time he enjoys running and jiu jitsu.

Vanta

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. Thousands of companies rely on Vanta to build, maintain and demonstrate trust in a way that's real-time and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, New York, San Francisco and Sydney.

REQUEST A DEMO

VANTA.COM