Galvanize
is now Diligent

Third-party risk management essentials

Table of contents

Third-party risk is everywhere

From big banks and university hospitals to retail fashion chains and every level of government, organizations around the world rely on third parties to provide products and services to keep them running effectively and efficiently. This is because outsourcing responsibilities to a third party helps you better serve customers, grow revenues and cut costs.

But bringing on third parties can also introduce a long list of risks that can do serious damage to an organization's financial and reputational well-being. (Like the real-life risk management disasters you'll read about later on.)

In this eBook, we'll discuss the basics of third-party risk management, how it differs from vendor risk management and how to begin the process of picking a risk management framework that best fits your organization.

What is third-party risk management?

ISACA[1] defines third-party risk management (TPRM) as **"The process of analyzing and controlling risks presented to your company, your data, your operations and your finances by parties other than your own company."**

Parties other than your own company are any non-customer entities that you've established a relationship with to outsource certain operational functions, or to source products or services. These entities are commonly referred to as third parties, vendors, suppliers, partners and business associates.

EXAMPLES OF THIRD-PARTY VENDORS:

+ Your office's paper shredding company
+ A contractor providing marketing services to your department
+ The food suppliers who stock your workplace cafeteria
+ The SaaS company that stores your data in the cloud

[1] *http://www.isaca.org/about-isaca*

Organizations' most critical risks

A global survey of 170 organizations[2] revealed their most critical risks:

1. Disruption in client service due to third-party action.

2. Breach of regulation or law by third parties.

3. Reputational damage.

4. Supply chain breakdown.

5. Financial fraud/exposure.

6. Failure of financial viability of a third party, impacting delivery.

Of the 170 global respondents:

1. 26% suffered reputational damage from third-party actions.

2. 23% have been non-compliant with regulatory requirements (8.7% of these faced a fine or financial penalty).

3. 23% have experienced financial- or transaction-reporting errors.

4. 20.6% have had sensitive customer data breached through third parties.

[2] **Deloitte,** *2016, Third-party governance and risk management, Extended enterprise risk management global survey*

So, how do third parties introduce risk?

Risk exposure begins when organizations give third-party vendors access to their facilities, networks and data—often with far less care and concern than they reserve for direct vendors. When one of your third-party vendors is compromised, your organization can experience devastating financial, reputational, regulatory, operational and strategic consequences. Even though your service provider made the mistake or is otherwise responsible, you'll still suffer the consequences. Your customers—and maybe even the courts—will hold your organization accountable.

In other words, a service can be outsourced, but risk ownership can't be.

So, if these are the consequences, then why don't organizations properly scrutinize their third-party vendors? Well, there are a number of potential reasons:

+ Teams and resources are already stretched to capacity
+ Other tasks are taking higher priority
+ There's an expectation that the third party itself is taking the necessary steps to manage risk
+ On average, companies share their data with 583 third parties,[3] creating serious complexity that many organizations just can't cope with
+ Uncertainty around how to implement a functioning vendor risk management (VRM) strategy and uncertainly about the true cost of ownership, which includes the logistics of ongoing maintenance and continual vendor assessment
+ There isn't buy-in from senior management, e.g., "We're not big enough to target" or "Nobody knows who we are"

[3] **Opus & Ponemon Institute,** *2018, Results of 2018 Third-Party Data Risk Study*

Real-world examples

Third-party failures have caused catastrophes in healthcare, banking, hospitality, manufacturing, retail and the public sector, and they continue to make front-page news, especially cybersecurity-related failures. Third parties are often the weakest link, making them much easier to target by cybercriminals. In fact, 63% of all cyberattacks could be traced either directly or indirectly to third parties.[4]

To prove that point, here are just a few third-party incidents that have gained international attention in recent years:

+ In 2014, 53 million email addresses and 56 million credit and debit card details were stolen from Home Depot, the largest home improvement retailer in the US. Hackers gained access to the credentials of a third-party vendor, eventually accessing the company's point-of-sale devices, where they deployed malware on self-checkout systems. The estimated cost of this data breach: $179 million, including a $25 million settlement.[5]
+ Marriott International, one of the largest hotel chains in the world, suffered a data breach in 2018. The company discovered that there had been unauthorized access by hackers through its Starwood guest reservation database system since 2014, exposing information such as the names, phone numbers, email addresses and passport numbers of nearly 400 million guests. The breach has cost Marriott $28 million to date; it is also facing a fine of $123 million for violating the European Commission General Data Protection Regulation.[6]

[4] **PwC,** *2018, The Global State of Information Security Survey*
[5] **Fortune,** *2017, Home Depot to pay banks $25 million in data breach settlement*
[6] **Forbes,** *2019, Marriott faces $123 million fine for 2018 mega-breach*

+ Capital One announced a third-party data breach that exposed the names, emails, addresses, phone numbers, birthdates and incomes of approximately 100 million Americans and 6 million Canadians. The company blamed a "configuration vulnerability" in the servers of the cloud computing company that hosted its customer data. According to Capital One in 2019, the breach could cost between $100 million and $150 million.[7]

While cybersecurity fails top the list, they're not the only thing that can take down an organization. For example, Chipotle suffered multiple food safety crises—yes, plural—in 2015. These were the result of a number of issues, including the decision to bring locally sourced food from various suppliers onto their menu. As a result, the company suffered six outbreaks of food-borne illness in 2015. The company's stock dropped 40%, and the company spent a hefty $50 million on marketing and promotion to win back customers.[8]

So whether it's a data breach, intellectual property theft or poor employee training, third-party mistakes are common (and costly).

Your third-party risk management program is only as strong as your weakest vendor.

» ***Chris Murphey, Director of Customer Success, Galvanize***

[7] **CNN,** *2019, A hacker gained access to 100 million Capital One credit card applications and accounts*
[8] **Risk Management Magazine,** *2016, Dia de la Crisis: The Chipotle outbreaks highlight supply chain risks*

The difference between VRM & TPRM

Before we dig deep into TPRM, we first need to address a very common question: “What’s the difference between vendor risk management (VRM) and third-party risk management (TPRM)?”

VRM is all about vetting partners, suppliers and vendors to make sure they meet certain conditions. These conditions, along with the expectations for each party, are detailed within the vendor contract, and include things like information security and regulatory compliance requirements. For example, you might specify how often a vendor audit needs to take place, or the password complexity requirements for anyone accessing your data.

TPRM goes even deeper and includes every single third party, like partners, government agencies, your franchises, or charities in which you donate your time or money, as well as all of your vendors. In this case, these organizations may require access to sensitive company data (e.g., to demonstrate compliance with government regulators), but you often have no ability to define who accesses it or how they use it—and there’s a good chance you can’t audit it.

TPRM often starts with VRM; it’s the foundation on which TPRM is built. Organizations will begin with a VRM program and, as they grow and mature, they’ll identify a need to address the specific and frequently disparate risks that a growing list of third parties present.

Whether you take a VRM or TPRM focus, ongoing monitoring of your program is essential. This is usually neglected as organizations settle into a long-term relationship with a vendor. But, as we’ve seen in our previous examples, not staying on top of these relationships and conditions only leads to trouble.

Fourth-party risk

If you think third parties are your only concern, we've got some bad news for you: You could be put at risk by your vendors' vendors—welcome to fourth-party risk. (And don't forget about your vendors' vendors' vendors... but we'll save fifth-party risk for another eBook.)

Fourth parties can introduce the same financial, reputational, regulatory, operational and strategic risks as third parties. However, fourth-party risk can be even more difficult to detect, manage and remediate, because you've got no legal contract with the organizations in this extended network.

In Deloitte's fourth annual extended enterprise risk management survey,[9] only 2% of respondents said they identify and monitor all fourth-party risks. And a further 8% only identify and monitor what they deem to be their most critical relationships.

Rather than being due to a lack of concern, this is often due to resource constraints. VRM teams struggle to manage their own vendors, making fourth-party risk management a seemingly insurmountable challenge. However, with increasing digital data exchange and improved AI and analytic capabilities, managing fourth-party risk will only get easier over time.

So, if fourth parties introduce just as much risk as third parties, how do you take a strategic approach to managing this?

Just like any risk program, TPRM should be linked to business objectives. You can take your direction by analyzing the organization's top risks, then link the risks posed by your third- and fourth-party vendors back to those organizational risks.

For example, if cybersecurity is one of your organization's top risks (and we hope it is), third parties who have access to your sensitive data will require deeper scrutiny and management than those who don't. This will flag organizations where you will require a deeper investigation into their subcontractors.

Again, we know that not all fourth parties can be managed the same way, but when it comes to your vendors, you can help protect and strengthen your organization by:

+ Taking a risk-aware approach to outsourcing services
+ Identifying and prioritizing risks based on organizational objectives
+ Creating detailed, legally binding contracts that include any and all vendor requirements (including fourth-party approvals for your most critical services)
+ Performing regular, ongoing assessments of your overall risk posture

These tasks can seem daunting, especially for organizations who are just entering this new stage of maturity—it's hard to know where to start. This is where using a purpose-built platform like ThirdPartyBond can help. Organizations can manage and automate the entire vendor risk process, minimizing the exposure to financial, operational, reputational and security risks from third parties—from third-party onboarding, assessment and remediation to performance monitoring and ongoing review, as well as termination.

[9] **Deloitte,** *2019, Fourth annual extended enterprise risk management survey*

How control frameworks help

When you're getting started with your TPRM program, the best place to begin is with the implementation of good governance. Part of this includes selecting and using control frameworks.

If you're not familiar with them, risk control frameworks help organizations build preventative and detective controls that are designed to mitigate risk to acceptable levels. They provide best practices and principles that result in a base level of assurance, and can be adapted to an organization's needs or specific requirements.

The two most common risk frameworks are the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).

NIST is available free of charge: https://doi.org/10.6028/NIST.CSWP.04162018. ISO frameworks can be purchased from their website: https://www.iso.org/. Many organizations, once they've established their initial framework, will expand and add other frameworks to make sure there aren't any gaps in risk coverage.

But, as you're probably not in the mood to read all 55 pages of NIST right now, here's a quick snapshot of the content you can expect.

FUNCTION	CATEGORY	SUBCATEGORY
Identify	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed and agreed to by organizational stakeholders. **ID.SC-2:** Suppliers and third-party partners of information systems, components and services are identified, prioritized and assessed using a cyber supply chain risk assessment process. **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test result or other forms of evaluations to confirm they are meeting their contractual obligations.

- **Function:** NIST defines five function areas: Identify, Protect, Detect, Respond and Recover
- **Category:** Actual controls are divided into categories; in the example on the previous page, it's Supply Chain Risk
- **Subcategory:** The subcategories detail the controls

So, while there's no one-size-fits-all framework, this provides a road map of sorts for organizations. It's an excellent starting point.

When deciding on your framework needs, it's important to consider the following:

- Regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS) and the *Health Insurance Portability and Accountability Act* (HIPAA)
- Compliance requirements (e.g., environmental, health and safety)
- Acceptable level of risk, defined by the probability and impact of a certain risk occurring
- Organizational objectives—otherwise, the priorities of individual departments may differ or conflict

These frameworks, combined with your specific organization's needs, can result in a lot of work. But there are software tools that can help you manage all of these requirements, controls and tasks. Our vendor risk management checklist can help you identify your needs and the software requirements to execute your program.

Galvanize case study

Large US healthcare provider automates manual, time-consuming vendor assessments

A large healthcare provider was conducting hundreds of assessments a year via email requests, manual surveys and spreadsheets. They were concerned, because they were only able to assess a small percentage of their vendor ecosystem using a manual process. Getting surveys completed properly and on time was a persistent challenge. If a vendor was considered a risk, the subsequent follow-up was very time-consuming.

The company wanted to automate the entire process: data gathering, notifications, risk scoring, analysis and remediation. Additionally, they wanted to integrate third-party intelligence so they could understand what happens if a vendor moves to a high-risk location or has financial viability issues. Finally, the company wanted to leverage their existing workflow processes and data from legacy systems.

The customer selected ThirdPartyBond, and the solution was implemented in three months. Since the assessment module went live, the company has increased the number of yearly assessments they were able to complete by 373%. If an assessment is determined to be low risk, ThirdPartyBond automatically generates a memo to internal stakeholders indicating the status. Meanwhile, high-risk assessments are escalated for action.

Conclusion

Third-party risks are only increasing, especially with more and more organizations relying on emerging technologies like cloud computing. Gartner estimates that, by 2020, 75% of Fortune Global 500 companies will treat vendor risk management as a board-level initiative to mitigate brand and reputation risk.

We hope this eBook has given you a foundational understanding of the complex world of third-party risk management.

Further learning & resources

Want to do some further reading? The following resources will provide you with more information on TPRM:

THIRD-PARTY RISK IS BECOMING A FIRST PRIORITY CHALLENGE

https://www2.deloitte.com/ca/en/pages/risk/articles/reduce-your-third-party-risk.html

THIRD-PARTY RISK MANAGEMENT

https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/the-practical-aspect-third-party-risk-management

GUIDANCE FOR MANAGING THIRD-PARTY RISK

https://www.fdic.gov/news/news/financial/2008/fil08044a.pdf

RISK MANAGEMENT IN THE REAL WORLD

https://www.charteredaccountants.ie/Accountancy-Ireland/Articles2/Leadership/Latest-News/Article-item/risk-management-in-the-real-world

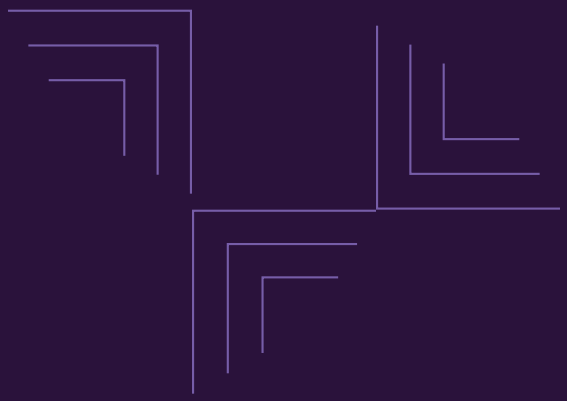
THIRD-PARTY RISK MANAGEMENT: KEEPING CONTROL IN A RAPIDLY CHANGING WORLD

https://eyfinancialservicesthoughtgallery.ie/third-party-risk-management-keeping-control-in-a-rapidly-changing-world/

Ready to find out how ThirdPartyBond helps manage third-party risk?

To find out how Galvanize can help your organization automate critical processes, deliver the answers that drive strategic change and improve your bottom line, call 1-888-669-4225, email info@wegalvanize.com or visit **wegalvanize.com**.

Galvanize
is now Diligent



ABOUT GALVANIZE

Galvanize, a Diligent brand, is the leading provider of GRC software for security, risk management, compliance and audit professionals. The integrated HighBond platform provides visibility into risk, makes it easy to demonstrate compliance, and helps grow audit, risk and compliance programs without incurring extra costs.

wegalvanize.com