CEP Magazine - December 2020
Collaboratively building effective third-party risk management processes

By Veronica Pickens, CHC

Veronica Pickens (vpickens@inovalon.com) is an Associate Vice President of Compliance and Delegation for Inovalon in Bowie, Maryland, USA.

- linkedin.com/in/veronica-pickens

Although the financial sector has been the leader in implementing third-party risk management processes, other sectors have understood its importance and followed suit. In the financial industry, the importance of third-party management was elevated in 2013 when the U.S. Office of the Comptroller of the Currency mandated that all regulated banks were required to manage the risk of their third parties.[1] The healthcare industry also has several regulations that led to the need for third-party management; the Health Insurance Portability and Accountability Act[2] sets the standard for protecting private patient data. Another example is the Health Information Technology for Economic and Clinical Health Act of 2009, which required increased privacy and security obligations and extended them to vendors who were classified as business associates of health insurance companies.[3]

However, for sectors without industry-specific regulations to drive a need for third-party management, effective practices had to be established. This article provides an introduction to the role of a third-party management program within an organization and an overview of best practices, emphasizing the importance of the program responsibilities being shared across departments.

The role of third-party risk management

Third-party risk management (TPRM) is the process of identifying, assessing, and controlling risks presented throughout the life cycle of an organization's relationship with any of its third parties (e.g., vendors, suppliers, distributors).[4] Organizations have to deal with their own internal risks, and when outsourcing or reliance on third parties are involved, organizations also have to understand the risks that those third parties have to minimize the impact. This often begins during the procurement process with third parties and should extend all the way through the end of the offboarding process. Risk types that are evaluated may include:

- **Strategic**: Risk that occurs due to adverse business decisions or the failure to implement appropriate business decisions in a manner consistent with stated strategic goals.
- **Reputational**: Risk that occurs due to negative public opinion of an organization.
- **Operational**: Risk that occurs due to loss created by inadequate or failed internal processes, people, systems, or external events.
- **Transactional**: Risk that occurs due to problems with service or product delivery.
- **Compliance**: Risk that occurs due to violations of laws, rules, or regulations; intentional and inadvertent

noncompliance with internal policies or procedures; or violations of the organization's business standards.

- **Information security**: Risk that occurs from unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information.

Things to consider when implementing a TPRM program

Implementing TPRM is not always an easy feat. Let us explore some common pitfalls of doing so.

Ineffective prioritization

Unfortunately, regulations only tell people what is required of them, not how to go about accomplishing the requirements. With this type of latitude, organizations can struggle with identifying the most optimal approach to managing their third-party relationships. This can also be compounded by the size of an organization and the difficulty in determining which departments need to be involved in the organization's TPRM program.

Departments that don't 'talk'

When organizations are too small, resource constraints are often inevitable, leading to ineffective TPRM; whereas when organizations are too large, there can be disjointed processes, and overmanagement of third-party relationships may occur. In these types of settings, often there is a multifunctional approach for managing such external relationships. Departments involved in the process may include compliance, delegation, enterprise procurement, security, and vendor management. Each of these departments may have some unique oversight requirements, but more often than not, there are some similar oversight needs. As such, how organizations go about accomplishing the oversight needs of their third-party relationships can lead to duplicative requests, ineffectiveness and inefficiency of their own resources, and overburdening of their third parties. This may become a vicious cycle for organizations, their third parties, and the third party's own business relationships.

Collaboration is key

These common pitfalls can be managed, but it takes collaborative efforts across multiple departments of an organization. Additionally, some of the pitfalls can be proactively and strategically addressed by ensuring that TPRM is part of an organization's enterprise risk management plan. Educating stakeholders on their roles in the TPRM process cycle and discussing up front what each department's oversight needs are can (1) lead to identifying commonality and (2) reveal the unique components that could lead to more efficient and effective initial due diligence and ongoing TPRM processes. It is important to remember that third-party relationships are ultimately extensions of an organization and can directly affect the organization, its customers, and its clients.

A collaborative effort is also important when organizations implement technology solutions to assist with their TPRM efforts. Any technology solution implemented should be designed and leveraged to support all of the organization's TPRM needs. Doing so helps facilitate cohesive management and intake of information that can be critically used across multiple functions to initially assess and manage third-party relationships on an ongoing basis and fully through the life cycle of those relationships. Furthermore, third parties will also appreciate potential streamlined processes versus having multiple clients and customers requesting duplicative information in the name of third-party oversight.

Lastly, this multifunctional, collaborative approach can be a win-win for all internal stakeholders by making the financial investment for technological and automated solutions more palatable, as the reach is across multiple business units/departments versus one functional area.

It takes a village

The days when TPRM processes were optional are long gone. Regulators continue to view third-party relationships as a high-risk area for organizations—one that must be appropriately managed. As recently demonstrated in the U.S. Department of Justice Criminal Division's update to its *Evaluation of Corporate Compliance Programs*, organizations must provide sufficient evidence of its TPRM processes from end to end.[5] Its expectation is that well-designed compliance programs are responsive and actively evaluate risk, and as such, third-party relationships are included as part of an organization's risk assessment.

It is, therefore, in the best interest of any organization that interacts with third parties to appropriately select those relationships in a manner that demonstrates sound due diligence processes and then manages them on an ongoing basis in support of its overall risk strategy. This should not be a disjointed or convoluted task. All functions involved in such processes should work collaboratively to help develop well-documented policies, processes, procedures, workflows, and systems to support these efforts effectively and efficiently, while establishing best practices and strong controls.

The views and opinions expressed in this article are those of the author and do not represent the views of the author's employer.

Takeaways

- Third-party management should be an essential component of any organization's risk strategy.
- There is increased regulatory scrutiny regarding how third-party relationships are selected and evaluated. Organizations will be penalized for not having the appropriate controls in place.
- Internal departments involved in the life cycle of third-party relationships should work together to create a strategic approach to managing these processes.
- Oversight processes for management of third-party relationships should be made to be both effective and efficient for both internal and external resources.
- Depending on an organization's breadth of third-party relationships, investing in technical and automated solutions may prove advantageous. The design and implementation should support cross-functional needs.

1 Office of the Comptroller of the Currency, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2013-29, October 30, 2013, https://bit.ly/34xJtL5.
2 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).
3 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, § 13,001, 123 Stat. 226 (2009).
4 Tom Rogers, "What is Third-Party Risk Management?" Vendor Centric (blog), March 7, 2019, https://bit.ly/34wPGH0.
5 U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated June 2020), http://bit.ly/2Z2Dp8R.