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.