Management Studies, Nov.-Dec. 2023, Vol. 11, No. 6, 307-311
doi: 10.17265/2328-2185/2023.06.001

Understanding the Importance of Effective Third-Party Risk Management on Data Governance

Marios E. Menexiadis
Aegean Airlines, Athens, Greece
National and Kapodistrian University of Athens, Athens, Greece
Michail Ch. Xanthopoulos
Aegean Airlines, Athens, Greece
University of Greenwich, London, UK

With a view to adopting to the globalized business landscape, organizations rely on third-party business relationships to enhance their operations, expand their capabilities, and drive innovation. While these collaborations offer numerous benefits, they also introduce a range of risks that organizations must carefully mitigate. If the obligation to meet the regulatory requirements is added to the equation, mitigating the third-party risk related to data governance, becomes one of the biggest challenges.

Keywords: third-party risk, data governance, data breach, internal control system, risk mitigation

Introduction

Third-party risk refers to the potential harm or negative impact that can arise from engaging with external entities, such as suppliers, vendors, contractors, business partners, or service providers. These risks can stem from several factors, including financial instability, operational vulnerabilities, regulatory non-compliance, security breaches, or unethical business practices.

Effectively managing third-party risk requires a comprehensive and systematic approach. Organizations need to establish robust processes, policies, and frameworks to evaluate and monitor the potential risks associated with their third-party relationships. This involves conducting thorough due diligence and risk assessments during the onboarding process and implementing ongoing monitoring mechanisms to identify emerging risks throughout the relationship lifecycle (Axson, 2010). Furthermore, organizations must establish clear contractual agreements that define the expectations, responsibilities, and liabilities of both parties. These agreements should address critical areas such as data protection, intellectual property rights, compliance with applicable regulations, business continuity planning, and incident response procedures (Bowman, 2023). Collaboration and communication play a crucial role in managing third-party risk. Organizations should foster open lines of communication with their

Marios E. Menexiadis, PhD, Group Internal Audit Director, Aegean Airlines, Athens, Greece; affiliate professor, department of Business Administration, National and Kapodistrian University of Athens, Athens, Greece.
Michail Ch. Xanthopoulos, MSc, Internal Auditor, Aegean Airlines, Athens, Greece; Global Shipping Management, University of Greenwich, London, UK.
Correspondence concerning this article should be addressed to Marios E. Menexiadis, National and Kapodistrian University of Athens, Athens, Greece.

third-party partners to ensure transparency, promote risk awareness, and facilitate the exchange of relevant information. Regular performance evaluations and audits should be conducted to assess the third party's adherence to established risk management practices and identify areas for improvement (Mishra, 2022).

Finally, organizations should have a robust incident response plan in place to effectively address and mitigate any potential risks or breaches that may occur. This plan should outline the necessary steps to be taken, the roles, and responsibilities of all stakeholders, and the communication channels to be activated in the event of a third-party-related incident. By adopting a proactive and holistic approach to managing third-party risk, organizations can strengthen their resilience, protect their assets, and maintain the trust of their stakeholders. It is a continuous process that requires ongoing vigilance, adaptability, and collaboration to navigate the evolving landscape of external relationships and safeguard the organization's interests in an increasingly interconnected world. Organizations specifically, are by definition material risk cases due to the complexity of the business.

Third Party-Risk Management and Data Governance

Third-party risk management in relation to data governance, refers to the process of identifying, assessing, mitigating, and monitoring risks associated with engaging external parties, such as vendors, suppliers, contractors, partners, or service providers, that have access to an organization's data, systems, or operations. It involves the evaluation of the potential risks that third parties pose and the implementation of measures that minimize those risks (Blokdyk, 2020). Third-party risk management has experienced significant changes and developments in recent years. Governments and regulatory authorities worldwide have recognized the importance of the effective risk management posed by third-party relationships and have consequently implemented regulations to safeguard organizations and their stakeholders.

Working with a third party can introduce risk to your business. However, if the latter has access to sensitive data, this can pose a security risk. If the third party provides a service for the business, then this leaves space for an operational risk. Risk discussions have a beginning but never an end, so this can go on and on. Third-party risk management is of extreme importance because it enables organizations to monitor and assess the risk posed by third parties to identify where it exceeds the threshold set by the business.

Third parties must have regular risk assessments performed by the organizations. These should be based on the area of risk posed by the third-party. The frequency of these assessments would be based on the tier, with the highest tier having the most frequent assessments.

It must never be forgotten that the third-party risk isn't stagnant, especially when it comes to data governance. New risks can emerge, while existing risks can evolve throughout the course of the business relationship.

Third parties should be continuously assessed, which ideally means monitoring for any changes in risk or performance. This can be done through more frequent assessments or external data feeds such as continuously updated cyber security ratings. Changes should automatically trigger an issue, assessment, and/or tier change. It is crucial to continuously monitor to ensure that all third parties are fulfilling their obligations and do not pose an undesirable risk to the organization (Simpson, 2018).

Third-Party Risk Management Metrics

The use of a third-party risk management program is quite important when mitigating the respective risk and its efficacy and achievement needs to be evaluated frequently. The complexity of third-party risk reporting arises from the need for these reports to be significant and add value for both the security team and the board.

The management of third parties inside businesses can be further complicated by the presence of extensive third-party networks, frequent changes, and limited resources.

However, regardless of the obstacles a company encounters, measures may be used to assess the efficacy of their management of third-party risk. There are two categories of metrics used in the realm of third-party risk management, namely key performance indicators (KPIs) and key risk indicators (KRIs) (Sabine, 2021).

Key Performance Indicators (KPIs) are used to assess the performance of the risk management team, while the Key Risk Indicators (KRIs) are used to quantify the inherent hazards associated with a particular situation or event. Key Risk Indicators (KRIs) serve as indicators of the level of risk associated with a particular activity and enable organizations to get a comprehensive understanding of their exposures to third-party risks.

These two metrics enable teams to simplify complex security procedures into easily comprehensible numerical values, so benefiting both the teams themselves and their governing bodies.

There are several approaches to properly report on third-party risks. The reporting of metrics to organizational boards varies depending on the manner in which a business engages with third parties and the associated risks they bring. Consequently, it is unlikely that two firms would adopt identical reporting approaches. The manner in which a risk team presents the respective findings to the board is significantly impacted by the level of security awareness possessed by the board members. Boards with less expertise may need a simplified set of criteria compared to boards that possess a comprehensive understanding of risk assessments. However, despite the potential variations in measurements, companies may adopt a standardized approach to determine the most suitable risk management measures for their specific needs. One recommended approach for selecting appropriate risk measurements is as follows.

To establish an effective risk program, it is recommended that risk teams include insights derived from various business units in order to develop a standardized approach. The potential results for any team may exhibit modest variations, nevertheless, this program aims to comprehensively outline the prerequisites of the business in effectively handling third-party risk during every stage of the third-party procedure.

Instead of rigidly establishing procedures or metrics (Zimmerbiomet, 2021), firms should see them as dynamic components of their risk program that may adapt to changes in the risk environment. The use of an always-on strategy facilitates the gradual development of metrics in tandem with the company, so assuring the firm’s sustained competitiveness amidst the dynamic landscape of threats.

The Road Ahead

Different perceptions exist on whose responsibility is the third-party risk on data governance. Although the risk and compliance officers think that it is the IT’s responsibility, the information security officers believe that it is the management’s responsibility to mitigate the respective risk. However, overall risk management is part of corporate governance and management should apply proper controls per risk case (Menexiadis, 2017). Proper risk management and effective controls is part of the internal control system. Consequently, it is not the IT’s responsibility to mitigate the third-party risk on data governance but the overall management’s.

Invest in Third-Party Risk Management Program

Organizations rely on third parties for many purposes as:

- For obtaining competitive advantage,
- For using skills and technologies to operate more effectively,

- For improvement in all aspects.

Although working with third parties offers numerous benefits, it also makes the organization vulnerable. Third parties have access to the organization's systems and sensitive data. Each third party has its own way and methodology for data-sharing, with various levels of security. However, there is no assurance that the third party is compliant with the regulations and the respective standards. It must never be forgotten that a wrong step, an incident may put compliance at risk, tarnish the organization's reputation, and negatively impact its performance. As mentioned above trainings are crucial at the daily life of the organization not only of their own employees, but also the ones of the third parties. Organizations need to consider potential threats across the business such as compliance, reputation, operations, cybersecurity.

However, threat monitoring is just one way technology can help the organization contain third-party risk (Johnsonlambert, 2023). It can also use a third-party risk management program to drive consistent and compliant performance from the third-party vendors. A robust third-party management program brings data together and delivers visibility into vendors' actions, to ensure compliance with all relevant regulations and laws. A third-party management program when managed properly through a unified platform, it helps keep every vendor aligned with your organization's goals, standards, and expectations.

Invest in Third-Party Risk Management Standards

McKinsey & Company in 2017, suggested that on a cross-industry basis, there is the opportunity to define common third-party risk management standards, which will set a course for a more secure and efficient future. They could also bring benefits such as an increase in cybersecurity and improved data management. They suggested that organizations should adopt strategies that reflect a systematic approach and help build a comprehensive framework.

Invest in Data Governance

Risks on third-party data governance are higher nowadays than ever before. Organizations operate in very complex environments, needless to say almost in digital ones. Big data is collected, stored, processed, and transferred across the industry globally. Organizations should comply with international standards, legislation, and regulations. Consequently, proper mitigation of third-party data governance is a necessity rather than a proper control to make the internal control system more effective.

References

Axson, D. A. J. (2010). *Best practices in planning and performance management.* Hoboken: Wiley.

Blokdyk, G. (2020). *Third party risk management framework: A complete guide* (2020 Edition). Queensland: Emereo Pty Limited.

Bowman, G. W. (2023). Privatizing correctional institutions. New York: Taylor & Francis.

Enforcementtracker. (2023). enforcementtracker. Retrieved from https://www.enforcementtracker.com/?insights

Johnsonlambert. (2023). Assess third party vendor risk with simple steps. Retrieved from https://www.johnsonlambert.com/insights/assess-third-party-vendor-risks/

Kezia, F. (2022). How the third-party risk management lifecycle can optimize your risk management program. Retrieved from https://www.diligent.com/resources/blog/third-party-risk-management-lifecycle

Mishra, A. (2022). *Modern cybersecurity strategies for enterprises*. Noida: BPB Publications.

Prevalent. (2023). *The 2023 third-party risk management study: How are organizations avoiding TPRM turbulence?* Definitive report.

Ryan, G., & Ortlieb, M. (2016). Sensitivity of personal data items in different online contexts. *Information Technology Journal Special Edition Usable Privacy and Security, 58*(5), 217-228.

Sabine, Z. (2021). TPRM metrics—Telling your risk story. Third party Risk Management. Shared assessment.

Tzanettis, I., Androna, M., Zafeiropoulos, A., Fotopoulou, E., & Papavassiliou, S. (2022). Data fusion of observability signals for assisting orchestration of distributed applications. *Sensors, 22*(5), 2061. Retrieved from https://doi.org/10.3390/s22052061

Vasileiou, D., Iriotis, N., Menexiadis, M., & Balios, D. (2017). *Internal audit in companies and organizations*. New York: Rossili Publications.

Wallis, T., Johnson, C., & Khamis, M. (2021). Interorganizational cooperation in supply chain cybersecurity: A cross-industry study of the effectiveness of the UK implementation of the NIS directive. *Information & Security, 48*, 36-68. doi:10.11610/isij.4812

Simpson, A. (2018). The role of transaction monitoring in ongoing monitoring: AML compliance programmes in Canada. *Journal of Financial Compliance, 2*(2), 165-175.

Zimmerbiomet. (2021). Zimmerbiomet.com. Retrieved from https://investor.zimmerbiomet.com/financial-information/annual-reports