Journal of Science and Technology
ISSN: 2456-5660 Volume 10, Issue 07 (July -2025)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2025.v10.i07.pp01- 09*

Contractual Agreement Aspect of Third-party Risk Management in Information Security

Ayoub Alfawzan, Omer Alrwais

King Saud University, Saudi Arabia

To Cite this Article

Ayoub Alfawzan, Omer Alrwais "**Contractual Agreement Aspect of Third-party Risk Management in Information Security**" *Journal of Science and Technology, Vol. 10, Issue 07-July 2025, pp01-09*

Article Info
Received: 20-04-2025 Revised: 20-06-2025 Accepted: 08-07-2025 Published:18 -07-2025

Abstract

Third-party risks are those faced by an organization when incorporating external entities into their ecosystem, infrastructure, or supply chains. These external parties may take the form of vendors, suppliers, partners, contractors, or service providers, all of whom are granted access to internal data concerning systems, processes, intellectual property, customer information, or internal communication. Organizations are reliant on outsourcing, subcontracting, and offshoring to support their business, this has amplified the need for effective Third-Party Risk Management (TPRM) frameworks. Although these practices offer operational efficiency, they introduce inherent risks, necessitating a careful approach to information security (IS). This article explores the pivotal role of contractual agreements in TPRM, addressing key questions about contract deficiencies, adaptability to evolving risks, regulatory impacts, and strategies for incentivizing third-party risk management. Thorough due diligence, collaborative approaches, and supplementary risk management strategies have been emphasized in the existing literature. The conceptual framework underscores the detrimental impact of weak contracts, advocating dynamic risk assessments, adaptable security standards, and communication and collaboration channels. Addressing variations in laws and regulations is crucial and requires a clear contractual provisions and language. The study concludes by providing insights into incentivizing third parties to adapt risk management practices and off-the-shelf tools and services handling, thereby contributing a comprehensive guide for organizations to manage third-party relationships in the domain of information security.

Keywords

Contracts, Contractual Agreement, Information Security, Third-Party Risk Management, Vendor.

Introduction

Outsourcing, sub-contracting, and offshoring are common practices carried out by many organizations, and organizations are increasingly dependent on vendors, partnerships, or the use of out-of-the-shelf tools to increase efficiency, reduce costs, and deliver quickly. This is done by all types of organizations working in different domains, whether it is a construction company depending on vendor to supply some materials, provider of health services outsourcing its laboratory, or a government entity developing a new program with a consultation company. Like everything in life, it comes with numerous benefits and introduces inherent risks to the organization.

Third-party risks are those faced by an organization when incorporating external entities into their ecosystem, infrastructure, or supply chains. These external parties may take the form of vendors, suppliers, partners, contractors, or service providers, all of whom are granted access to internal data concerning systems, processes, intellectual property, customer information, or internal communication. An essential consideration regarding external entities is that despite having robust risk management and risk management strategies within the organization, the same standards may not be consistently upheld by external partners. This dynamic introduces a potential for vulnerabilities in risk management, even within an organization with the strongest controls.The concept of third-party risk management (TPRM) was formed to manage and govern the risks accompanying these relationships with external parties. TPRM anticipates, detects, assesses, reduces, and resolves the risks associated with dealing with vendors, partnerships, or the use of off-the-shelf services and tools.

In information security (IS), TPRM mainly focuses on the risks associated with introducing external entities into the organization, and involves identifying, evaluating, and mitigating potential IS risks raised from given access to information technology resources to those external parties, or the use of external services and tools. These third parties may not comply with the same policies, standards, and guidelines of the organization; this will create a gap in the overall IS governance of the organization unless the relationships are handled at the same level. TPRM in IS encompasses several key components, including conducting a thorough risk assessment to evaluate the potential security risks created by third parties on the organization’s information system or their capabilities to secure the services they provide to the organization. Additionally, the organization should conduct its due diligence on the security practices of third parties and their compliance with security regulations before entering partnerships or deciding to use their services. This should include audits, security assessments, and continuous reviews of third-party policies and procedures. Furthermore, TPRM includes establishing clear expectations and requirements related to IS through contractual agreements and specifying measures such as data protection, incident response procedures, and compliance obligations. The contract is a way to ensure that the third party matches the organization’s IS strategy, policies, standards, and guidelines; this will reduce the risks from third parties to the same levels of the organization’s risk appetite.

Problem Statement

As organizations increasingly rely on third parties, managing the risks associated with these relationships has become a critical concern. Although TPRM has gained attention, a thorough understanding of the role of contractual agreements in TPRM is still lacking. These agreements are crucial for effective TPRM, but their intricacies, shortcomings, and potential improvements require further examination. Contractual agreements are the foundation for establishing clear expectations, defining responsibilities, and outlining risk-mitigation strategies between the organization and its third-party partners. The efficacy of TPRM is inherently linked to the thoroughness, transparency, and enforceability of these contracts. The type of contract used varies, depending on the nature of the relationship between the parties involved. For instance, online tools demand different contracts compared to in-house off-the-shelf tools. Similarly, outsourcing application operations require a distinct contract structure compared to managing it internally using contractors.

This study aims to address the following key questions:

- How do the flaws and weaknesses in contractual agreements with third parties increase the overall risk for the organization?
- To what degree do contractual agreements address the evolving nature of third-party risk?
- How do variations in regulations and standards impact the development and enforcement of contractual agreements?
- What are the best practices and strategies that an organization can employ to leverage agreements to incentivize third-party partners to adopt strong risk management practices?

Related Work

The Contractual Agreement Aspect of Third-party Risk Management within the domain of information security has gained attention from researchers, with many studies addressing the topic and many others studying risk management in general. This review summarizes some of the most important findings of these studies and discusses how contractual agreements can be used to reduce information security risks in third-party relationships.

Sharing an organization’s data or infrastructure with vendors to perform its functions requires thorough due diligence to protect the organization against possible risk exposure (Singh, 2009). Identifying key stakeholders and their roles and responsibilities within the organization to ensure that all security requirements and activities are part of the contract while negotiating the contract with vendors should be part of any new agreements with third parties (Singh, 2009).

Contracts with third parties are important because they establish the terms and conditions of the relationship between the organization and third party. They can help clarify expectations, responsibilities, and liabilities and can provide a framework for managing risks associated with outsourcing. However, even well-drafted contracts may not fully protect the organization from third-party risks, as outsourcing inherently means that the organization depends on external entities with different approaches to resilience and cybersecurity. Therefore, it is important to supplement contracts with other risk management strategies such as due diligence, monitoring, and contingency planning, which should be incorporated into the contract (Haller & Wallen, 2016).

Identifying relevant information security legal requirements imposed by laws and regulatory requirements on the organization is the first step in writing a contract. Additionally, the level of compliance should be decided and mentioned in words that match the official wording to avoid any ambiguities. Subsequently, other requirements specific to the project or the organization can be identified and agreed to with its responsibilities and how to monitor and measure it (Bomhard, 2021).

Conceptual Framework of Contractual Agreements in TPRM

Weak Contracts

Organizations face adverse challenges and increased overall risk dealing with third parties with a weak contract, particularly those that fail to comprehensively cover information security requirements associated with what the third party is doing, creating a precarious environment with potential ramifications for the organization's operational resilience and data protection measures.

Contracts lacking coverage of information security requirements may unintentionally create significant gaps in the protection of sensitive organizational information. Failure to explicitly outline security measures, protocols, and standards leaves room for oversight, thereby increasing the likelihood of vulnerabilities that malicious actors may exploit. Consequently, organizations become more susceptible to data breaches, unauthorized access, and other security incidents. Moreover, compliance deficiencies became more pronounced. Organizations operating in regulated industries or subject to data protection laws require explicit contractual stipulations to ensure adherence to legal frameworks. Failure to address these aspects in contracts can lead to unintentional non-compliance, exposing the organization to regulatory penalties and legal repercussions.

Contracts with language ambiguities or imprecise terminology create an environment in which the responsibility allocation is unclear. The lack of specificity regarding the party that is accountable for various aspects of information security introduces ambiguity, making it challenging to enforce adherence to security measures. This ambiguity extends to incident responses, data handling procedures, and other critical security domains, heightening the organization's vulnerability. Additionally, the continuous process of identifying new risks and mitigating them will not be handled, which will cause the organization to face all types of new risks in the evolving information technology world.

Failure to consult legal and security departments during contract negotiations can result in misalignments between contractual provisions and established security policies. Contracts should be seamlessly integrated with an organization's security policies to ensure a coherent and robust security posture. When this alignment is lacking, the organization faces the risk of noncompliance with its own security standards, diminishing the effectiveness of its overall security strategy. Additionally, the contract lacks comprehensive remediation measures. In the event of a security incident, the absence of clear contractual provisions may hinder the organization's ability to promptly address and rectify breaches. This, in turn, prolongs the exposure to potential damages and exacerbates the impact on the organization's reputation.

Weak contracts may impede effective vendor management strategies. Without well-defined information security requirements, organizations struggle to hold third-party vendors accountable to a standard that aligns with their security objectives. This, in turn, hinders the establishment of strategic partnerships with vendors who can actively contribute to the organization's overarching security goals.

Evolving Risks

Currently, information security risks evolve at the same rate as information technology, and contemporary organizational risk management should adapt quickly to change. Thus, contractual agreements with third parties are essential for shaping the resilience of organizations against emerging risks. Key factors influence the efficacy of these contracts in addressing the dynamic nature of risk. Dynamic risk assessment provisions are included in contracts to address these risks efficiently. These provisions acknowledge that security measures must be routinely reviewed and adjusted to respond to new threats. Such a contractual language guarantees that information security processes remain current and efficient for the duration of a contract.

An effective contractual agreement incorporates adaptable security standards and protocols to recognize the dynamic nature of information security. Instead of having rigid, one-size-fits-all security requirements, agreements should be sufficiently flexible to adapt to changes in technology, best practices, and regulatory environments. In addition, provisions for continuous monitoring and reporting are included along with requirements to update them, which enable organizations to receive real-time insight into security practices, promptly identify emerging risks, and allow updates to such mechanisms. This flexibility guarantees that security measures remain in line with the state of the threat landscape and strengthen the organization’s ability to proactively respond to evolving threats.

Third-party risk is dynamic, in part due to changing laws and regulatory requirements. Effective contracts show that they are aware of these developments and contain clauses requiring adherence to newly established or updated legal and regulatory obligations. This ensures that organizations and their third parties stay up-to-date and minimize legal and compliance risks.

To effectively manage the dynamic nature of risk, contractual agreements must include collaboration and communication channels. Contracts should specify how information will be exchanged between the organization and its vendors in a timely manner, facilitating a proactive and cooperative approach to identifying, assessing, and mitigating emerging risks. These channels should enable swift and coordinated response to security incidents.

Variants Laws and Regulations

Variations in information security laws and regulations heavily impact the development and enforcement of contractual agreements between organizations and third parties. When structuring and negotiating agreements with third-party entities, organizations must navigate the complex and frequently divergent laws and regulations requirements. Contracts must take into consideration the variations across jurisdictions and industry regulators in order to guarantee compliance. Contracts must comply with all applicable laws in the area where the organization and third-party entities conduct their business. Failure to do so, these variations may expose the organization to the legal risks of fines, penalties, and, most importantly, reputational damage.

Considering the various privacy and data protection regulations that apply to different areas and sectors is essential. Contracts have to contain clauses that strictly adhere to the guidelines and standards provided by the relevant data protection laws. These guidelines should cover the data handling, processing, storage, and transfer mechanisms. Furthermore, a customized strategy is needed because of the dynamic nature of industry-specific security requirements, and agreements should be carefully crafted to closely follow industry-specific best practices. To maintain regulatory compliance and uphold the highest standards of security, whether operating in healthcare, finance, or any other sector, a nuanced understanding of and integration with sector-specific security requirements is imperative.

Interaction with both national and international cybersecurity frameworks adds another level of complexity. These frameworks provide directions for information system security, influencing the selection of the required security controls, risk assessment methodologies, and incident response protocols. To improve an organization's overall risk exposure, contracts should specifically mention and correspond to established cybersecurity frameworks. Furthermore, the need for contracts to define liability and accountability precisely is highlighted by the differences in these aspects, which are frequently determined by jurisdiction-specific regulations. Contracts must carefully manage regional variations in liability allocation to prevent disagreements and legal challenges and guarantee a robust and legally compliant basis for information security collaborations.

Incentivize Risk Management

Allowing contracts to encourage third parties to implement strong information security and risk-management procedures requires a methodical and comprehensive approach. The cornerstone is found in the contract's precise definition of the strict security requirements. Commitment to high security standards is encouraged and measurable targets are established by integrating performance metrics and service-level agreements linked to security measures. This also provides a foundation for performance-based incentives. Third parties are encouraged to invest in strong security measures in order to avoid financial penalties for noncompliance. Additionally, organizations should include clauses in contracts that require ongoing security assessments, audits, and monitoring. Working together on joint exercises, simulations, and incident response planning improves the readiness of the third-party. A culture of continuous improvement is promoted when excellent security practices are acknowledged and rewarded, whether through financial incentives or favorable mentions in reviews. Moreover, incorporating provisions that allow for security upgrades and setting up procedures for regular evaluation and modification guarantees that contractual incentives remain in line with the ever-changing nature of information security, encouraging a proactive and flexible approach to risk management.

Off-the-shelf Tools and Services

The use of off-the-shelf tools and services with non-negotiable terms and conditions requires different handling methods. Thorough evaluation of the vendor and the tool or service, taking into account aspects like reputation, security protocols, and compliance with industry standards. Careful examination of the predefined terms is crucial, ensuring that the organization's policies and standards are followed, or at least the minimum acceptable version may be applicable. Ensure that the service complies with industry regulations and applicable laws. Furthermore, make use of any security measures and settings that are present in the tool or service in order to customize it to match the organization's security policies.

Concurrently, strong monitoring systems are implemented to trace the tool's behavior, create a customized incident response strategy, and routinely assess the security procedures and performance of the vendor. Periodically review alternative tolls to stay up-to-date on new options that better suit the organization's security and risk management needs. Establish internal guidelines for the safe use of such tools and services, train employees in safe procedures, and establish explicit escalation protocols for pressing problems.

Conclusion

In conclusion, given the increasing use of outsourcing, subcontracting, and offshoring in today's organizational operations, a careful approach to Third-Party Risk Management (TPRM) is required. These practices have inherent risks, in addition to their intrinsic benefits, which makes a strong TPRM framework necessary. In this context, information security (IS) is crucial, with an emphasis on minimizing risks related to services performed by external entities and assuring their compliance with internal governance. Contractual agreements serve as the cornerstone of effective TPRM, providing a framework for clear expectations, assigned responsibilities, and risk mitigation strategies.

The issues identified with current TPRM practices revolve around the lack of an in-depth understanding of the role of contractual agreements. This article covers important questions about contract defects, contract flexibility in the face of changing risks, the effect of regulations, and methods to encourage third-party partners to adopt strong risk management practices. Previous studies have emphasized the importance of thorough due diligence, teamwork, and the addition of supplementary risk management techniques to contracts. Effective contract negotiations must consider legal requirements, compliance, and language clarity.

The conceptual framework of contractual agreements in TPRM emphasizes the detrimental impact of weak contracts on overall organizational risk. Ambiguities, lack of consultation, and inadequate remediation measures create vulnerabilities that hinder effective vendor management. The evolving nature of risks necessitates dynamic risk assessment provisions, adaptable security standards, and collaborative channels in contracts. Variations in laws and regulations underscore the need for nuanced, industry-specific contractual language. This study provides insights into incentivizing risk management through precise contractual definitions, performance metrics, and collaborative exercises.

To address the challenges posed by off-the-shelf tools and services, organizations must conduct thorough evaluations, adhere to predefined terms, and leverage the available security measures. Establishing internal guidelines, training programs, and escalation protocols further enhances the safe utilization of these tools. Overall, this research contributes to a comprehensive understanding of the contractual agreement aspect in TPRM, offering valuable insights and recommendations for organizations navigating the complex landscape of third-party relationships in the realm of information security.

References

Aris, S. R. H. S., Arshad, N. H., & Mohamed, A. (2008). Conceptual framework on risk management in IT outsourcing projects. management, 36(37), 37-38.

Bhatti, B. M., Mubarak, S., & Nagalingam, S. (2021). Information security risk management in it outsourcing–a quarter-century systematic literature review. Journal of Global Information Technology Management, 24(4), 259-298.

Boggavarapu, S. (2021). The Effect of Third-Party Service Providers on Information Security Breaches at Financial Institutions (Doctoral dissertation, University of the Cumberlands).

Bomhard, D., & Daum, A. (2021). Cybersecurity in outsourcing and cloud computing: a growing challenge for contract drafting, International Cybersecurity Law Review, 2(1), 161-171.

Haller, J., & Wallen, C. (2016). Managing Third Party Risk in Financial Services Organizations: A Resilience-Based Approach, Carnegie Mellon University Software Engineering Institute.

Singh, A. (2009). Improving Information Security Risk Management [Unpublished doctoral dissertation]. University of Minnesota.

VanHoy, J. (2021). Third Party Risk Management. Available at SSRN 3763399.