World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies

Oluwatosin Ilori [1, *], Nelly Tochi Nwosu [2] and Henry Nwapali Ndidi Naiho [3]

[1] *Independent Researcher, Irving, TX, USA.*
[2] *Independent Researcher, Chicago, IL, USA.*
[3] *Independent Researcher, New York, USA.*

World Journal of Advanced Research and Reviews, 2024, 22(03), 213–224

Publication history: Received on 26 April 2024; revised on 04 June 2024; accepted on 06 June 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.3.1727

Abstract

In the increasingly interconnected digital landscape, third-party vendors play a critical role in providing essential services and capabilities to organizations. However, these external partnerships also introduce significant IT security risks, making it imperative for organizations to implement robust strategies for managing third-party vendor risks. This paper provides a comprehensive audit review of third-party vendor risks in IT security and outlines effective mitigation strategies. The audit review identifies key risk areas associated with third-party vendors, including data breaches, inadequate security controls, and compliance issues. Real-world case studies highlight the severe consequences of insufficient vendor risk management, such as substantial financial losses, reputational damage, and regulatory penalties. Through these examples, the review underscores the critical need for organizations to prioritize vendor risk management in their IT security frameworks. Recommended mitigation strategies are detailed, focusing on enhancing security controls, implementing regular security assessments, and establishing clear contractual agreements. Enhancing security controls involves rigorous vetting of vendors, enforcing strong authentication and encryption protocols, and ensuring vendors adhere to the organization's security policies. Regular security assessments, including audits and penetration testing, are crucial for identifying vulnerabilities and ensuring continuous compliance with security standards. Establishing clear contractual agreements with vendors helps define security expectations, responsibilities, and penalties for non-compliance, thereby creating a legal framework that supports robust risk management. The importance of continuous monitoring and oversight is emphasized, highlighting that effective third-party risk management is not a one-time activity but an ongoing process. Continuous monitoring involves real-time tracking of vendor performance and security posture, supported by automated tools and regular audits to promptly address emerging threats. This paper concludes by stressing the necessity for organizations to adopt a proactive approach to third-party vendor risk management, integrating it as a core component of their overall IT security strategy. By doing so, organizations can mitigate the risks associated with third-party vendors, protect sensitive data, and ensure compliance with regulatory requirements, ultimately safeguarding their operations and reputation in the digital age.

Keywords: Third-Party; Vendor Risks; IT Security; Mitigation Strategies; Audit Review

1. Introduction

In today's interconnected business environment, organizations increasingly rely on third-party vendors to provide essential services, software, and infrastructure. While these partnerships offer significant benefits, including cost savings, specialized expertise, and operational efficiencies, they also introduce substantial risks to IT security. Third-party vendors can be potential points of vulnerability, exposing organizations to data breaches, cyber-attacks, and compliance failures (Adama & Okeke, 2024, Jejeniwa, Mhlongo & Jejeniwa, 2024). These risks are compounded by the

[*] Corresponding author: Oluwatosin Ilori

Copyright © 2024 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

complexity and opacity of modern supply chains, where vendors may have access to sensitive information and critical systems. Third-party vendor risks in IT security encompass a range of threats, including inadequate security measures by the vendor, insufficient oversight and control mechanisms, and the potential for malicious insiders within the vendor organization. The increasing prevalence of cyber-attacks targeting supply chains has highlighted the urgent need for robust risk management strategies to safeguard organizational assets and maintain regulatory compliance.

Auditing third-party vendors is a critical component of a comprehensive IT security strategy. Effective audits help organizations identify and assess the security practices of their vendors, ensuring that they meet the necessary standards and comply with regulatory requirements (Popoola, et. Al., 2024, Uzougbo, Ikegwu & Adewusi, 2024). Regular audits provide visibility into the vendor's security posture, highlight potential vulnerabilities, and facilitate proactive risk mitigation measures. Mitigating third-party vendor risks is essential to protect sensitive data, maintain business continuity, and uphold an organization's reputation (Adegbola, et. al., 2024, Jejeniwa, Mhlongo & Jejeniwa, 2024). Failure to address these risks can result in significant financial losses, legal penalties, and damage to stakeholder trust. As regulatory bodies increasingly emphasize the importance of third-party risk management, organizations must prioritize robust auditing and risk mitigation strategies to avoid compliance issues and safeguard their operations.

This paper aims to provide a comprehensive review of third-party vendor risks in IT security and outline effective audit and mitigation strategies. The purpose is to equip organizations with the knowledge and tools needed to manage these risks effectively, ensuring the security and integrity of their IT environments. An in-depth examination of the types of risks posed by third-party vendors, including common vulnerabilities and threat vectors. A review of established frameworks and best practices for conducting thorough and effective audits of third-party vendors. This will include guidelines on audit planning, execution, and reporting. Detailed strategies for mitigating identified risks, including contractual safeguards, continuous monitoring, and incident response planning.

Analysis of real-world incidents involving third-party vendor risks, highlighting lessons learned and successful mitigation efforts. Insights into emerging trends and future threats in third-party vendor risk management, along with recommendations for staying ahead of these challenges (Edu, et. al., 2022, Nnaji, et. al., 2024). By exploring these areas, the paper will provide a comprehensive understanding of third-party vendor risks in IT security and offer practical guidance for organizations to enhance their risk management practices. This will ultimately contribute to more resilient and secure IT ecosystems, capable of withstanding the complexities and threats of modern supply chains.

1.1. Third-Party Vendor Risks

Third-party vendor risks pose significant challenges to organizations across various industries. These risks encompass a range of potential threats, including data breaches, supply chain attacks, and compliance failures, each with its own set of implications for organizational security and operational integrity (Adama & Okeke, 2024, Popoola, et. Al., 2024). Data breaches are one of the most prevalent risks associated with third-party vendors. These breaches can occur when vendors fail to implement robust security measures, leading to unauthorized access to sensitive information. The impact of a data breach can be severe, resulting in financial losses, reputational damage, and legal repercussions. Organizations must therefore ensure that their vendors adhere to strict data protection standards and implement adequate security measures to mitigate the risk of breaches.

Supply chain attacks are another significant risk posed by third-party vendors. These attacks involve exploiting vulnerabilities in the supply chain to gain unauthorized access to an organization's systems or data (Benjamin, Amajuoyi & Adeusi, 2024, Jejeniwa, Mhlongo & Jejeniwa, 2024). By compromising a trusted vendor, attackers can infiltrate an organization's network and launch sophisticated attacks, such as malware infections or data exfiltration. The impact of a successful supply chain attack can be devastating, leading to widespread disruption and financial loss. Organizations must therefore conduct thorough risk assessments of their supply chain partners and implement robust security controls to mitigate this risk. Compliance failures are also a major concern when it comes to third-party vendor risks. Many organizations rely on third-party vendors to perform critical functions, such as payment processing or data storage, which are subject to regulatory requirements. If a vendor fails to comply with these requirements, it can expose the organization to regulatory sanctions, fines, and legal action. Organizations must therefore ensure that their vendors adhere to relevant regulations and industry standards to avoid compliance failures.

The impact of these risks on organizations can be significant (Adama & Okeke, 2024, Nnaji, et. al., 2024). Beyond the immediate financial and reputational costs associated with breaches, attacks, or compliance failures, organizations may also face operational disruptions, loss of customer trust, and legal liabilities. Therefore, it is essential for organizations to proactively manage third-party vendor risks by implementing robust risk management processes, conducting regular audits and assessments, and fostering a culture of security and compliance throughout the organization. In addition to the risks mentioned earlier, third-party vendor risks can also include: If a third-party vendor is involved in a scandal or data breach, it can reflect poorly on the organization that contracted them, leading to a loss of trust among customers, partners, and stakeholders. Dependence on third-party vendors for critical services or products can lead to operational disruptions if the vendor fails to deliver as expected (Ikegwu, et. al., 2017, Jejeniwa, Mhlongo & Jejeniwa, 2024). This can impact the organization's ability to conduct business smoothly and efficiently. Contracting with unreliable or financially unstable vendors can lead to financial losses if the vendor goes out of business or fails to deliver on their obligations. This can result in additional costs to find alternative vendors or solutions.

If a third-party vendor fails to comply with applicable laws and regulations, the organization that contracted them may also be held liable. This can result in regulatory fines, penalties, and legal action (Adama, et. al., 2024, Popoola, et. Al., 2024). Third-party vendors may introduce cybersecurity vulnerabilities into an organization's network or systems. This can be due to insecure software, inadequate security practices, or a lack of awareness about cybersecurity risks. To mitigate these risks, organizations should conduct thorough due diligence when selecting third-party vendors, including assessing their financial stability, security practices, compliance with regulations, and reputation. Additionally, organizations should establish clear contractual agreements with vendors that outline expectations, responsibilities, and liability in the event of a breach or other issue. Regular monitoring and audits of third-party vendors can also help ensure ongoing compliance and reduce the risk of negative impacts on the organization.

1.2. Audit Review Process

In today's interconnected business environment, organizations rely heavily on third-party vendors to support their IT infrastructure and services. However, with this reliance comes inherent risks, particularly in the realm of cybersecurity (Adama, et. al., 2024, Nnaji, et. al., 2024). Conducting comprehensive audit reviews of third-party vendors is crucial to identify and mitigate potential risks effectively. Here's an overview of the audit review process: Begin by conducting a thorough risk assessment to identify the critical vendors and the potential risks associated with their services or products. This assessment should consider factors such as the sensitivity of the data or systems involved, the vendor's access privileges, and their security practices.

Establish criteria for selecting vendors and perform due diligence checks before engaging with them. This includes evaluating their security policies, compliance with regulations, financial stability, and previous track record (Ikegwu, et. al., 2022, Uzougbo, Ikegwu & Adewusi, 2024). Develop a detailed audit plan outlining the objectives, scope, and approach of the audit. Consider factors such as the type of services provided by the vendor, the level of access they have to sensitive data, and any regulatory requirements that apply. Conduct on-site visits or remote audits to assess the vendor's IT security controls, processes, and procedures. This may involve reviewing documentation, interviewing key personnel, and performing technical assessments of their systems. Document all findings, observations, and recommendations resulting from the audit. Prepare a comprehensive audit report highlighting areas of strength, weaknesses, and opportunities for improvement. Ensure that the report is clear, concise, and actionable (Adegbola, et. al., 2024, Jejeniwa, Mhlongo & Jejeniwa, 2024). Evaluate the effectiveness of the vendor's security controls, including access controls, encryption mechanisms, intrusion detection systems, and incident response procedures. Assess how the vendor handles sensitive data, including data encryption, data storage practices, data retention policies, and data transfer mechanisms. Ensure that the vendor complies with relevant regulations and industry standards, such as GDPR, HIPAA, PCI DSS, and ISO 27001. Review the vendor's business continuity and disaster recovery plans to ensure that they have measures in place to mitigate the impact of potential disruptions.

COBIT provides a comprehensive framework for governing and managing enterprise IT. It can be used to establish controls and assess the effectiveness of IT processes within both the organization and its third-party vendors (Adama, et. al., 2024, Nnaji, et. al., 2024). ITIL offers best practices for IT service management and can help organizations and their vendors improve the quality and efficiency of IT service delivery. It provides guidance on areas such as service design, transition, operation, and continual improvement. By following a structured audit review process and leveraging established standards and frameworks, organizations can effectively assess and manage the risks associated with third-party vendors in IT security. This proactive approach helps enhance cybersecurity resilience and safeguard the organization's assets, reputation, and stakeholders' trust.

Work with the vendor to develop and implement risk mitigation plans based on audit findings. These plans should address identified weaknesses and include specific actions, timelines, and responsibilities (Adeusi, Jejeniwa & Jejeniwa, 2024, Uzougbo, Ikegwu & Adewusi, 2024). Ensure that contracts with vendors include specific clauses related to security requirements, compliance with laws and regulations, data protection, and breach notification procedures. Establish mechanisms for ongoing monitoring and oversight of vendor activities, including regular audits, performance reviews, and security assessments. Provide training and raise awareness among employees about the risks associated with third-party vendors and the importance of following security protocols.

Establish a feedback loop to capture lessons learned from audits and use them to improve future audit processes and vendor management practices. Conduct regular reviews of vendor relationships to ensure that they continue to meet security and compliance requirements (Adama, et. al., 2024, Popoola, et. Al., 2024). Stay agile and adapt audit processes and strategies to address emerging risks and changes in the IT landscape. Collaborate with industry peers and share best practices for auditing third-party vendors to strengthen overall cybersecurity resilience. Participate in information sharing platforms and forums to stay informed about the latest threats and vulnerabilities affecting third-party vendors. By implementing these strategies, organizations can effectively manage and mitigate the risks associated with third-party vendors in IT security, ensuring the integrity and security of their systems and data.

1.3. Identified Risks

During audits of third-party vendors in IT security, several risks and vulnerabilities are often uncovered. These risks can vary in nature and severity but generally pose significant threats to the organization's cybersecurity posture and data integrity (Nnaji, et. al., 2024, Uzougbo, Ikegwu & Adewusi, 2024). Vendors may have inadequate security measures in place, leading to the risk of data breaches and unauthorized access to sensitive information. Weaknesses in a vendor's supply chain management processes can expose organizations to supply chain attacks, where malicious actors target vulnerabilities in third-party vendors to infiltrate the organization's systems. Vendors may fail to comply with regulatory requirements and industry standards, exposing the organization to legal and reputational risks. Poor access control mechanisms can result in unauthorized access to systems and data, increasing the risk of insider threats and data leakage.

Some vendors may not provide sufficient transparency into their security practices and processes, making it challenging for organizations to assess and mitigate risks effectively (Jejeniwa, Mhlongo & Jejeniwa, 2024, Uzougbo, Ikegwu & Adewusi, 2024). Organizations may become overly dependent on certain vendors, increasing their exposure to risks if those vendors experience disruptions or security breaches. Inadequate oversight of vendor activities and relationships can result in gaps in security and compliance, leaving the organization vulnerable to various risks. Limited resources, such as budget and manpower, may hinder organizations' ability to effectively audit and mitigate third-party vendor risks.

Identifying and addressing these risks is crucial for organizations to enhance their cybersecurity resilience and protect sensitive data from potential threats posed by third-party vendors. Third-party vendors may lack robust security controls, such as encryption, multifactor authentication, and regular security assessments, increasing the risk of data breaches and cyberattacks (Jejeniwa, Mhlongo & Jejeniwa, 2024). Inadequate incident response planning by vendors can result in delays in detecting and mitigating security incidents, leading to prolonged data exposure and damage to the organization's reputation. Vendors may not have effective data loss prevention measures in place, increasing the risk of data leakage and unauthorized disclosure of sensitive information. Organizations may fail to conduct thorough due diligence when selecting and onboarding vendors, leading to the engagement of high-risk vendors with inadequate security practices. Vendors may not have robust business continuity and disaster recovery plans, increasing the risk of disruptions to critical services and operations.

Conduct comprehensive risk assessments of third-party vendors, considering factors such as security practices, compliance with regulations, and the sensitivity of the data they handle. Include specific security requirements and responsibilities in vendor contracts, such as data protection measures, incident response procedures, and compliance with industry standards. Regularly monitor and audit third-party vendors to ensure compliance with security requirements and identify any emerging risks or vulnerabilities. Provide security awareness training to vendors and their employees to enhance their understanding of cybersecurity best practices and threat mitigation strategies. Implement strong encryption protocols and access controls to protect sensitive data from unauthorized access and disclosure (Uzougbo, Ikegwu & Adewusi, 2024). Develop and maintain robust incident response plans in collaboration with vendors to ensure timely detection, containment, and mitigation of security incidents. Conduct regular security assessments, such as penetration testing and vulnerability scanning, to identify and address potential security weaknesses in vendor systems and applications. Ensure that vendors have effective business continuity and disaster recovery plans in place to minimize the impact of disruptions on critical services and operations.

1.4. Mitigation Strategies

In today's interconnected digital landscape, businesses often rely on third-party vendors to provide various services and products (Raftari, 2022, Thomas & Sule, 2023, Tyaliti, 2023). While this can lead to increased efficiency and innovation, it also introduces significant cybersecurity risks. Third-party vendors may have access to sensitive data or systems, making them potential targets for cyberattacks. To mitigate these risks, it is crucial for organizations to implement robust strategies that enhance security controls, conduct regular security assessments, and establish clear contractual agreements. Additionally, continuous monitoring and oversight are essential to ensure that vendors comply with security requirements and promptly address any potential vulnerabilities.

One of the most effective ways to mitigate third-party vendor risks is to enhance security controls. This includes implementing strong authentication measures, such as multi-factor authentication, to verify the identity of individuals accessing systems or data. Additionally, organizations should enforce strict access controls to limit the data and systems that vendors can access. Regular security audits and vulnerability assessments can help identify and mitigate potential security gaps. Regular security assessments are essential to ensure that third-party vendors comply with security requirements and best practices (Billio, et. al., 2021, Edunjobi, 2024, Shet, et. al., 2021). These assessments should include thorough evaluations of vendors' security policies, procedures, and infrastructure. Organizations should also conduct penetration testing and vulnerability scans to identify and remediate potential security vulnerabilities. Regular audits can help ensure that vendors are implementing effective security controls and adhering to contractual agreements.

Clear contractual agreements are essential for mitigating third-party vendor risks. Contracts should clearly outline the security requirements that vendors must adhere to, including data protection measures, incident response procedures, and breach notification requirements (Anagnostopoulos, 2018, Gomber, et. al., 2018, Verma & Gustafsson, 2020). Contracts should also specify the scope of services provided by vendors, the duration of the agreement, and the process for terminating the agreement. By establishing clear contractual agreements, organizations can hold vendors accountable for maintaining a high level of security. Continuous monitoring and oversight are critical components of an effective third-party vendor risk management program (Fatima & Elbanna, 2023, Jan, Lai & Tahir, 2021, Ogundipe, Odejide & Edunjobi, 2024). By continuously monitoring vendors' activities and performance, organizations can quickly identify and address potential security issues. Continuous monitoring can include regular security audits, real-time monitoring of network traffic, and ongoing evaluation of vendors' compliance with security requirements. Oversight should involve regular reviews of vendors' security policies and procedures, as well as regular communication and collaboration with vendors to ensure that they understand and comply with security requirements. Additionally, organizations should conduct regular risk assessments to identify and prioritize potential security risks associated with third-party vendors.

In conclusion, mitigating third-party vendor risks in IT security requires a comprehensive approach that includes enhancing security controls, implementing regular security assessments, and establishing clear contractual agreements. Continuous monitoring and oversight are essential to ensure that vendors comply with security requirements and promptly address any potential vulnerabilities (Abdulrasool & Turnbull, 2020, Nzeako, et. al., 2024, Suresh, Varalakshmi & Chand, 2024). By implementing these strategies, organizations can effectively mitigate the risks associated with third-party vendors and protect their sensitive data and systems. Mitigation Strategies of Third-Party Vendor Risks in IT Security: A Comprehensive Audit Review and Mitigation Strategies. In the realm of IT security, third-party vendors play a significant role in providing essential services and technologies to organizations. However, this reliance on external parties introduces a host of cybersecurity risks that must be effectively managed and mitigated. A comprehensive audit review coupled with proactive mitigation strategies is crucial to address these risks and safeguard sensitive data and systems. Strengthening security controls is paramount in mitigating third-party vendor risks. Organizations should enforce robust authentication mechanisms, such as biometric verification or token-based authentication, to ensure that only authorized personnel can access critical systems and data (Moullin, et. al., 2020, Zabolotniaia, et. al., 2020). Implementing encryption protocols for data in transit and at rest can further protect against unauthorized access. Regular security audits and vulnerability assessments should be conducted to identify and remediate potential security gaps.

Regular security assessments are essential to evaluate third-party vendors' adherence to security standards and best practices. These assessments should encompass a thorough review of vendors' security policies, procedures, and infrastructure. Penetration testing and vulnerability scans can help identify and mitigate potential security vulnerabilities. Organizations should also ensure that vendors undergo regular audits to verify compliance with security requirements and contractual agreements. Clear and concise contractual agreements are crucial in mitigating third-party vendor risks. Contracts should outline specific security requirements, including data protection measures, incident response protocols, and breach notification procedures (AlGhamdi, Win & Vlahu-Gjorgievska, 2020, Shaw, 2020, Wong, 2022). Additionally, contracts should specify the scope of services provided by vendors, the duration of the agreement, and the process for terminating the agreement. By establishing clear contractual agreements, organizations can hold vendors accountable for maintaining a high level of security.

Continuous monitoring and oversight are essential components of an effective third-party vendor risk management strategy. By continuously monitoring vendors' activities and performance, organizations can quickly detect and respond to potential security incidents (Levstek, Pucihar & Hovelja, 2022, Obazu, 2020, Yeboah-Ofori & Opoku-Boateng, 2023). Real-time monitoring of network traffic and regular reviews of vendors' security policies and procedures can help ensure compliance with security requirements. Ongoing communication and collaboration with vendors are also crucial to address any emerging security threats promptly. In conclusion, mitigating third-party vendor risks in IT security requires a comprehensive approach that includes enhancing security controls, implementing regular security assessments, and establishing clear contractual agreements. Continuous monitoring and oversight are essential to ensure that vendors comply with security requirements and promptly address any potential vulnerabilities. By adopting these strategies, organizations can effectively mitigate the risks associated with third-party vendors and protect their sensitive data and systems.

2. Case Studies

In 2013, Target experienced a massive data breach that compromised the personal and financial information of over 110 million customers. The breach was initiated through a third-party vendor, an HVAC contractor, whose credentials were stolen and used to access Target's network (Attaran, 2020, Baran & Woznyj, 2020, Van Greuning & Bratanovic, 2020). This breach resulted in significant financial losses for Target, including settlements with affected customers and regulatory fines. In 2017, Equifax, one of the largest credit reporting agencies, suffered a data breach that exposed the personal information of approximately 147 million consumers. The breach was attributed to a vulnerability in a third-party software tool used by Equifax. This breach had severe consequences for Equifax, including a drop in stock value, numerous lawsuits, and reputational damage.

In 2014, Home Depot experienced a data breach that affected around 56 million payment cards. The breach was attributed to malware that was introduced into Home Depot's systems through a third-party vendor's credentials (Moudoubah, et. al., 2021, Rusman, Nadlifatin & Subriadi, 2022, Saeedinezhad, Naghsh & Peikari, 2021). The breach resulted in significant financial losses for Home Depot, including costs associated with fraud losses and legal settlements. These case studies highlight the importance of robust vendor risk management practices. Organizations should conduct thorough due diligence before engaging third-party vendors, including assessing their security practices and conducting regular audits and assessments.

To prevent unauthorized access through compromised credentials, organizations should implement multi-factor authentication (MFA) for accessing sensitive systems and data. This can significantly reduce the risk of credential theft (Amorim, et. al., 2021, Makaš, 2023, Turak, 2024). Continuous monitoring of network traffic and systems can help detect and respond to unauthorized access or suspicious activities promptly. Implementing intrusion detection and prevention systems can aid in early detection of potential security breaches. Clear and comprehensive contractual agreements should be established with third-party vendors, outlining security requirements, data protection measures, incident response procedures, and breach notification requirements. These agreements should also include provisions for regular security audits and assessments. These case studies underscore the importance of proactive risk management and security practices when engaging third-party vendors. By implementing robust security controls, conducting regular assessments, and establishing clear contractual agreements, organizations can mitigate the risks associated with third-party vendors and protect their sensitive data and systems.

In 2016, Uber experienced a data breach that affected 57 million users and drivers. The breach occurred due to hackers gaining access to Uber's GitHub account, where they found credentials to Uber's AWS account (Dwivedi, Alabdooli & Dwivedi, 2021, Keiningham, et. al., 2020). This breach highlighted the risks associated with third-party vendors and the importance of securing all access points to sensitive data. In 2018, it was revealed that Cambridge Analytica, a third-party data analytics firm, had improperly accessed and used the personal data of 87 million Facebook users. This incident raised concerns about the lack of oversight and control over third-party vendors' use of data and led to increased scrutiny of data sharing practices. In 2018, British Airways suffered a data breach that affected 500,000 customers. The breach was attributed to malicious code injected into the airline's website, which harvested customer data and sent it to an external server. This incident highlighted the importance of monitoring and securing all access points to prevent unauthorized access. Organizations should implement robust vendor oversight mechanisms, including regular audits, security assessments, and monitoring of third-party vendors' activities.

Organizations should adopt a data minimization approach, only sharing and providing access to third-party vendors with the minimum amount of data necessary for them to perform their services (Karo & Faza, 2023, Mengistu, 2020, Otto, 2020). Organizations should have a comprehensive incident response plan in place to quickly detect, respond to, and mitigate the impact of data breaches or security incidents involving third-party vendors. Organizations should prioritize transparency and accountability in their relationships with third-party vendors, ensuring that vendors adhere to agreed-upon security practices and contractual obligations. In conclusion, these case studies underscore the importance of implementing robust security measures and oversight mechanisms when engaging third-party vendors. By learning from these examples and implementing proactive risk management strategies, organizations can mitigate the risks associated with third-party vendors and protect their sensitive data and systems.

3. Best Practices

Before engaging a third-party vendor, conduct a comprehensive assessment of their security practices, including their data protection measures, incident response procedures, and compliance with relevant regulations (Mahalle, Yong & Tao, 2020, Yandri, Utama & Zahra, 2019). Establish clear and concise contractual agreements that outline the security requirements, data protection measures, and breach notification procedures that vendors must adhere to. Ensure that third-party vendors undergo regular security audits and assessments to identify and mitigate potential security vulnerabilities. Limit the access that third-party vendors have to sensitive systems and data to minimize the risk of unauthorized access. Implement monitoring tools and intrusion detection systems to detect and respond to unauthorized access or suspicious activities promptly.

Establish a cybersecurity policy that outlines the organization's security objectives, roles and responsibilities, and incident response procedures. Use a combination of security measures, such as firewalls, antivirus software, and encryption, to protect against various types of cyber threats (Abdulrasool & Turnbull, 2020, Marchão, Reis & Ventura, 2020, Nachrowi, Nurhadryani & Sukoco, 2020). Provide regular training and awareness programs to employees and third-party vendors to educate them about cybersecurity best practices and the importance of data protection. Ensure that all systems and software are regularly updated and patched to protect against known vulnerabilities. Develop an incident response plan that outlines the steps to be taken in the event of a data breach or security incident, including communication with affected parties and regulatory authorities. By implementing these best practices and strategies, organizations can effectively manage third-party vendor risks in IT security and build a resilient cybersecurity framework to protect against cyber threats.

Regularly monitor third-party vendors' activities and performance to ensure compliance with security requirements and promptly address any potential vulnerabilities. Require third-party vendors to use MFA for accessing sensitive systems and data to reduce the risk of unauthorized access (Al Faruq, et. al., 2020, Bin Ahmad, Ibrahim & Bin Ngah, 2020, Samiei & Habibi, 2021). Require third-party vendors to encrypt sensitive data both in transit and at rest to protect against data breaches. Provide regular security training to third-party vendors to ensure they are aware of the latest security threats and best practices. Establish clear lines of communication and coordination for incident response between the organization and third-party vendors to facilitate a swift and effective response to security incidents. Identify and prioritize cybersecurity risks based on their potential impact on the organization and implement appropriate mitigation measures. Conduct regular security assessments, including penetration testing and vulnerability scans, to identify and address potential security vulnerabilities (Al Faruq, et. al., 2020, Bin Ahmad, Ibrahim & Bin Ngah, 2020, Samiei & Habibi, 2021). Ensure that secure coding practices are followed throughout the software development lifecycle to reduce the risk of vulnerabilities in software applications. Regularly test the organization's incident response plan through tabletop exercises and simulations to ensure its effectiveness in responding to security incidents. Foster a culture of cybersecurity awareness within the organization by providing regular training and encouraging employees to report suspicious activities. By incorporating these best practices and strategies into their cybersecurity framework, organizations can effectively manage third-party vendor risks in IT security and enhance their overall cybersecurity posture.

4. Conclusion

In conclusion, managing third-party vendor risks in IT security is critical for organizations to protect their sensitive data and systems from cyber threats. Through a comprehensive audit review and the implementation of mitigation strategies, organizations can significantly reduce the risk of data breaches and security incidents. Key findings from this study include the importance of conducting thorough due diligence when engaging third-party vendors, implementing strong contractual agreements that outline security requirements, and regularly monitoring vendors' activities and performance. Additionally, strategies such as enhancing security controls, implementing multi-factor authentication, and conducting regular security assessments can help mitigate third-party vendor risks effectively.

Organizations must prioritize third-party vendor risk management to safeguard their operations and reputation. It is essential to establish a robust cybersecurity framework that includes clear policies, regular assessments, and continuous monitoring of third-party vendors. By implementing best practices and strategies outlined in this study, organizations can strengthen their cybersecurity posture and mitigate the risks associated with third-party vendors. Looking ahead, the future of third-party vendor risk management will likely focus on automation and artificial intelligence (AI) to enhance security controls and monitoring capabilities. Organizations may also increasingly rely on blockchain technology to secure and verify transactions with third-party vendors. Additionally, regulatory requirements around data protection and privacy are expected to continue to evolve, requiring organizations to adapt their risk management practices accordingly. In conclusion, third-party vendor risk management is a complex and evolving discipline that requires continuous attention and adaptation. By staying informed about emerging trends and best practices, organizations can effectively mitigate third-party vendor risks and protect their critical assets.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Reference

[1] Abdulrasool, F. E., & Turnbull, S. J. (2020). Exploring security, risk, and compliance driven IT governance model for universities: applied research based on the COBIT framework. *International Journal of Electronic Banking*, *2*(3), 237-265.

[2] Abdulrasool, F. E., & Turnbull, S. J. (2020). Exploring security, risk, and compliance driven IT governance model for universities: applied research based on the COBIT framework. *International Journal of Electronic Banking*, *2*(3), 237-265.

[3] Adama, H. E., & Okeke, C. D. (2024). Comparative analysis and implementation of a transformative business and supply chain model for the FMCG sector in Africa and the USA. Magna Scientia Advanced Research and Reviews, 10(02), 265–271. DOI: https://doi.org/10.30574/msarr.2024.10.2.0067

[4] Adama, H. E., & Okeke, C. D. (2024). Digital transformation as a catalyst for business model innovation: A critical review of impact and implementation strategies. Magna Scientia Advanced Research and Reviews, 10(02), 256–264. DOI: https://doi.org/10.30574/msarr.2024.10.2.0066

[5] Adama, H. E., & Okeke, C. D. (2024). Harnessing business analytics for gaining competitive advantage in emerging markets: A systematic review of approaches and outcomes. International Journal of Science and Research Archive, 11(02), 1848–1854. DOI: https://doi.org/10.30574/ijsra.2024.11.2.0683

[6] Adama, H. E., Popoola, O. A., Okeke, C. D., & Akinoso, A. E. (2024). Theoretical frameworks supporting IT and business strategy alignment for sustained competitive advantage. International Journal of Management & Entrepreneurship Research, 6(4), 1273-1287. DOI: 10.51594/ijmer.v6i4.1058. Fair East Publishers. Retrieved from http://www.fepbl.com/index.php/ijmer

[7] Adama, H. E., Popoola, O. A., Okeke, C. D., & Akinoso, A. E. (2024). Economic theory and practical impacts of digital transformation in supply chain optimization. International Journal of Advanced Economics, 6(4), 95-107. DOI: 10.51594/ijae.v6i4.1072. Fair East Publishers. Retrieved from http://www.fepbl.com/index.php/ijae

[8] Adama, H.E., Popoola, O.A., Okeke, C.D. and Akinoso, A.E. (2024). Theoretical Frameworks Supporting IT and Business Strategy Alignment for Sustained Competitive Advantage. International Journal of Management & Entrepreneurship Research, 6(4), pp.1273-1287.

[9] Adama, H.E., Popoola, O.A., Okeke, C.D. and Akinoso, A.E. (2024). Economic Theory and Practical Impacts of Digital Transformation in Supply Chain Optimization. International Journal of Advanced Economics, 6(4), pp.95-107

[10] Adegbola, A. E., Adegbola, M. D., Amajuoyi, P., Benjamin, L. B., & Adeusi, K. B. (2024). Fostering product development efficiency through cross-functional team leadership: Insights and strategies from industry experts. *International Journal of Management & Entrepreneurship Research*, *6*(5), 1733-1753.

[11] Adegbola, M. D., Adegbola, A. E., Amajuoyi, P., Benjamin, L. B., & Adeusi, K. B. (2024). Leveraging financial incentives for enhanced diversity: A review and new models. *International Journal of Applied Research in Social Sciences*, *6*(5), 1037-1047.

[12] Al Faruq, B., Herlianto, H. R., Simbolon, S. H., Utama, D. N., & Wibowo, A. (2020). Integration of ITIL V3, ISO 20000 & iso 27001: 2013forit services and security management system. *International Journal*, *9*(3).

[13] AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, *99*, 102030.

[14] Amorim, A. C., da Silva, M. M., Pereira, R., & Gonçalves, M. (2021). Using agile methodologies for adopting COBIT. *Information Systems*, *101*, 101496.

[15] Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business*, *100*, 7-25.

[16] Attaran, M. (2020, July). Digital technology enablers and their implications for supply chain management. In *Supply Chain Forum: An International Journal* (Vol. 21, No. 3, pp. 158-172). Taylor & Francis.

[17] Baran, B. E., & Woznyj, H. M. (2020). Managing VUCA: The human dynamics of agility. *Organizational dynamics*.

[18] Benjamin, L. B., Amajuoyi, P., & Adeusi, K. B. (2024). Marketing, communication, banking, and Fintech: personalization in Fintech marketing, enhancing customer communication for financial inclusion. *International Journal of Management & Entrepreneurship Research*, *6*(5), 1687-1701.

[19] Bhatt, U., Antorán, J., Zhang, Y., Liao, Q. V., Sattigeri, P., Fogliato, R., ... & Xiang, A. (2021, July). Uncertainty as a form of transparency: Measuring, communicating, and using uncertainty. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 401-413).

[20] Billio, M., Costola, M., Hristova, I., Latino, C., & Pelizzon, L. (2021). Inside the ESG ratings:(Dis) agreement and performance. *Corporate Social Responsibility and Environmental Management*, *28*(5), 1426-1445.

[21] bin Ahmad, A., Ibrahim, I., & bin Ngah, L. (2020). A review of service quality elements towards the overlapping IT framework process on the IT hardware support services (ITHS). *International Journal*, *9*(1.4).

[22] Dwivedi, P., Alabdooli, J. I., & Dwivedi, R. (2021). Role of FinTech adoption for competitiveness and performance of the bank: a study of banking industry in UAE. *International Journal of Global Business and Competitiveness*, *16*(2), 130-138.

[23] Edu, Y., Eimunjeze, J., Onah, P., Adedoyin, D., David, P.O., Ikegwu, C. Fintech Update: SEC New Rules On The Issuance, Offering Platforms and Custody of Digital Assets- What You need to Know. Mondaq (July 6, 2022)

[24] Edunjobi, T. E. (2024). Sustainable supply chain financing models: Integrating banking for enhanced sustainability. *International Journal for Multidisciplinary Research Updates 2024*, *7*(02), 001-011.

[25] Fatima, T., & Elbanna, S. (2023). Corporate social responsibility (CSR) implementation: A review and a research agenda towards an integrative framework. *Journal of Business Ethics*, *183*(1), 105-121.

[26] Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards transparency by design for artificial intelligence. *Science and engineering ethics*, *26*(6), 3333-3361.

[27] Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of management information systems*, *35*(1), 220-265.

[28] Hyland-Wood, B., Gardner, J., Leask, J., & Ecker, U. K. (2021). Toward effective government communication strategies in the era of COVID-19. *Humanities and Social Sciences Communications*, *8*(1), 1-11.

[29] Ikegwu, C., An Appraisal of Technological Advancement in The Nigerian Legal System. ABUAD Law Students' Society Journal (ALSSJ) Apr. 24, 2017

[30] Ikegwu, C.G., Governance Challenges Faced by the Bitcoin Ecosystem: The Way Forward. Social Science Research Network Journal (December 22, 2022)

[31] Jan, A. A., Lai, F. W., & Tahir, M. (2021). Developing an Islamic Corporate Governance framework to examine sustainability performance in Islamic Banks and Financial Institutions. *Journal of Cleaner Production*, *315*, 128099.

[32] Karo, T. A. K., & Faza, A. (2023). Evaluation of Integration and Human Resources in Information Technology Governance using COBIT 2019: PT. Pelabuhan Indonesia Tanjung Priok Branch. *Journal of Information Systems and Informatics*, *5*(3), 902-914.

[33] KB Adeusi, TO Jejeniwa, TO Jejeniwa (2024) Advancing financial transparency and ethical governance: innovation cost management and accountability in higher education and industry. International Journal of Management & Entrepreneurship Research 6 (5), 1533-1546

[34] Keiningham, T., Aksoy, L., Bruce, H. L., Cadet, F., Clennell, N., Hodgkinson, I. R., & Kearney, T. (2020). Customer experience driven business model innovation. *Journal of Business Research*, *116*, 431-440.

[35] Levstek, A., Pucihar, A., & Hovelja, T. (2022). Towards an adaptive strategic IT governance model for SMEs. *Journal of theoretical and applied electronic commerce research*, *17*(1), 230-252.

[36] Mahalle, A., Yong, J., & Tao, X. (2020, January). ITIL process management to mitigate operations risk in cloud architecture infrastructure for banking and financial services industry. In *Web Intelligence* (Vol. 18, No. 3, pp. 229-238). IOS Press.

[37] Makaš, A. (2023). Governance, risk and compliance frameworks applicability in the organizations. *International Journal of Science and Research Archive*, *10*(2), 716-724.

[38] Marchão, J., Reis, L., & Ventura, P. (2020, October). Operation management using ITIL and COBIT framework. In *Conference Proceedings (part of ITEMA conference collection)* (pp. 201-207).

[39] Mengistu, F. M. (2020). *IT SERVICE MANAGEMENT AGILITY ASSESSMENT MODEL: THE CASE OF CBE* (Doctoral dissertation, ADDIS ABABA UNIVERSITY).

[40] Moudoubah, L., El Yamami, A., Mansouri, K., & Qbadou, M. (2021). From IT service management to IT service governance: An ontological approach for integrated use of ITIL and COBIT frameworks. *International Journal of Electrical and Computer Engineering*, *11*(6), 5292.

[41] Moullin, J. C., Dickson, K. S., Stadnick, N. A., Becan, J. E., Wiley, T., Phillips, J., ... & Aarons, G. A. (2020). Exploration, preparation, implementation, sustainment (EPIS) framework. *Handbook on implementation science*, 32-61.

[42] Mvelase, N. (2022). *IT service management best practices in insurance industries* (Doctoral dissertation, University of Johannesburg).

[43] Nachrowi, E., Nurhadryani, Y., & Sukoco, H. (2020). Evaluation of governance and management of information technology services using Cobit 2019 and ITIL 4. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(4), 764-774.

[44] Nnaji, U. O., Benjamin, L. B., Eyo-Udo, N. L., & Augustine, E. (2024). A review of strategic decision-making in marketing through big data and analytics.

[45] Nnaji, U. O., Benjamin, L. B., Eyo-Udo, N. L., & Augustine, E. (2024). Advanced risk management models for supply chain finance.

[46] Nnaji, U. O., Benjamin, L. B., Eyo-Udo, N. L., & Etukudoh, E. A. (2024). Strategies for enhancing global supply chain resilience to climate change. *International Journal of Management & Entrepreneurship Research*, *6*(5), 1677-1686.

[47] Nnaji, U. O., Benjamin, L. B., Eyo-Udo, N. L., & Etukudoh, E. A. (2024). Effective cost management strategies in global supply chains. *International Journal of Applied Research in Social Sciences*, *6*(5), 945-953.

[48] Nnaji, U. O., Benjamin, L. B., Eyo-Udo, N. L., & Etukudoh, E. A. (2024). Incorporating sustainable engineering practices into supply chain management for environmental impact reduction. *GSC Advanced Research and Reviews*, *19*(2), 138-143.

[49] Nzeako, G., Akinsanya, M. O., Popoola, O. A., Chukwurah, E. G., Okeke, C. D., & Akpukorji, I. S. (2024). Theoretical insights into IT governance and compliance in banking: Perspectives from African and US regulatory environments. *International Journal of Management & Entrepreneurship Research*, *6*(5), 1457-1466.

[50] Obazu, I. D. (2020). *Information Technology Infrastructure Library: Postimplementation Experiences of Small Business IT Support Employees* (Doctoral dissertation, Walden University).

[51] Ogundipe, D. O., Odejide, O. A., & Edunjobi, T. E. (2024). Agile methodologies in digital banking: Theoretical underpinnings and implications for custom satisfaction. *Open Access Research Journal of Science and Technology*, *10*(02), 021-030.

[52] Otto, L. (2020). IT-Governance in Integrated Care: A Risk-centred Examination in Germany. In *HEALTHINF* (pp. 808-817).

[53] Popoola, O. A., Adama, H. E., Okeke, C. D., & Akinoso, A. E. (2024). The strategic value of business analysts in enhancing organizational efficiency and operations. International Journal of Management & Entrepreneurship Research, 6(4), 1288-1303. DOI: 10.51594/ijmer.v6i4.1059. Fair East Publishers. Retrieved from http://www.fepbl.com/index.php/ijmer

[54] Popoola, O. A., Adama, H. E., Okeke, C. D., & Akinoso, A. E. (2024). Cross-industry frameworks for business process reengineering: Conceptual models and practical executions. World Journal of Advanced Research and Reviews, 22(01), 1198–1208. DOI: 10.30574/wjarr.2024.22.1.1201. https://doi.org/10.30574/wjarr.2024.22.1.1201

[55] Popoola, O. A., Adama, H. E., Okeke, C. D., & Akinoso, A. E. (2024). Conceptualizing agile development in digital transformations: Theoretical foundations and practical applications. Engineering Science & Technology Journal, 5(4), 1524-1541. DOI: 10.51594/estj/v5i4.1080. Fair East Publishers. Retrieved from http://www.fepbl.com/index.php/estj

[56] Popoola, O. A., Adama, H. E., Okeke, C. D., & Akinoso, A. E. (2024). Advancements and innovations in requirements elicitation: Developing a comprehensive conceptual model. World Journal of Advanced Research and Reviews, 22(01), 1209–1220. DOI: https://doi.org/10.30574/wjarr.2024.22.1.1202

[57] Raftari, A. (2022). *Framework for Evaluation of Blockchain-AI Technology and Governance to Secure Interoperable US Healthcare Data* (Doctoral dissertation, Northcentral University).

[58] Rusman, A., Nadlifatin, R., & Subriadi, A. P. (2022). Information System Audit Using COBIT and ITIL Framework: Literature Review. *Sinkron: jurnal dan penelitian teknik informatika*, *7*(3), 799-810.

[59] Saeedinezhad, S., Naghsh, A., & Peikari, H. R. (2021). A Framework for Implementing IT Service Management in the Field of Pre-hospital Emergency Management with an Integrated Approach COBIT Maturity Model and ITIL Framework. *Health Management & Information Science*, *8*(1), 53-67.

[60] Samiei, E., & Habibi, J. (2021). Toward a Comprehensive IT Management Methodology. *IEEE Engineering Management Review*, *50*(1), 168-185.

[61] Shaw, K. (2020). *Prioritizing Information Technology Infrastructure Library (ITIL) Implementations and Identifying Critical Success Factors to Improve the Probability of Success* (Doctoral dissertation, Capella University).

[62] Shet, S. V., Poddar, T., Samuel, F. W., & Dwivedi, Y. K. (2021). Examining the determinants of successful adoption of data analytics in human resource management–A framework for implications. *Journal of Business Research*, *131*, 311-326.

[63] Suresh, M. N., Varalakshmi, T., & Chand, M. S. (2024). IT Governance Framework Ensuring Effective Management and Compliance. *International Research Journal on Advanced Engineering and Management (IRJAEM)*, *2*(05), 1627-1632.

[64] Thomas, G., & Sule, M. J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(1), 18-40.

[65] TO Jejeniwa, NZ Mhlongo, TO Jejeniwa (2024) A comprehensive review of the impact of artificial intelligence on modern accounting practices and financial reporting. Computer Science & IT Research Journal 5 (4), 1031-1047

[66] TO Jejeniwa, NZ Mhlongo, TO Jejeniwa (2024) AI solutions for developmental economics: opportunities and challenges in financial inclusion and poverty alleviation. International Journal of Advanced Economics 6 (4), 108-123

[67] TO Jejeniwa, NZ Mhlongo, TO Jejeniwa (2024) Conceptualizing e-government initiatives: lessons learned from Africa-US collaborations in digital governance. International Journal of Applied Research in Social Sciences 6 (4), 759-769

[68] TO Jejeniwa, NZ Mhlongo, TO Jejeniwa (2024) Diversity and inclusion in the workplace: a conceptual framework comparing the USA and Nigeria. International Journal of Management & Entrepreneurship Research 6 (5), 1368-1394

[69] TO Jejeniwa, NZ Mhlongo, TO Jejeniwa (2024) Social impact of automated accounting systems: a review: analyzing the societal and employment implications of the rapid digitization in the accounting industry. Finance

& Accounting Research Journal 6 (4), 684-706

[70] TO Jejeniwa, NZ Mhlongo, TO Jejeniwa (2024) The role of ethical practices in accounting: A review of corporate governance and compliance trends. Finance & Accounting Research Journal 6 (4), 707-720

[71] TO Jejeniwa, NZ Mhlongo, TO Jejeniwa (2024) Theoretical perspectives on digital transformation in financial services: insights from case studies in Africa and the United States. Finance & Accounting Research Journal 6 (4), 674-683

[72] Turak, F. (2024). *IT governance and digital transformation: assessing governance contingencies in large Finnish banks with COBIT 2019* (Bachelor's thesis).

[73] Tyaliti, S. P. (2023). *Effects of Rapid Technology Advancement (RTA) on IT-audit skills and competencies within the financial services sector in South* (Doctoral dissertation, Cape Peninsula University of Technology).

[74] Uzougbo, N.S., Ikegwu, C.G., & Adewusi, A.O. Cybersecurity Compliance in Financial Institutions: A Comparative Analysis of Global Standards and Regulations. International Journal of Science and Research Archive, 12(01), pp. 533-548

[75] Uzougbo, N.S., Ikegwu, C.G., & Adewusi, A.O. Enhancing Consumer Protection in Cryptocurrency Transactions: Legal Strategies and Policy Recommendations. International Journal of Science and Research Archive, 12(01), pp. 520-532

[76] Uzougbo, N.S., Ikegwu, C.G., & Adewusi, A.O. International Enforcement of Cryptocurrency Laws: Jurisdictional Challenges and Collaborative Solutions. Magna Scientia Advanced Research and Reviews, 11(01), pp. 068-083

[77] Uzougbo, N.S., Ikegwu, C.G., & Adewusi, A.O. Legal Accountability and Ethical Considerations of AI in Financial Services. GSC Advanced Research and Reviews, 19(02), pp. 130–142

[78] Uzougbo, N.S., Ikegwu, C.G., & Adewusi, A.O. Regulatory Frameworks For Decentralized Finance (DeFi): Challenges and Opportunities. GSC Advanced Research and Reviews, 19(02), pp. 116–129

[79] Valackiene, A., & Andrijauskaite, R. (2021). Model for Assessing Information Logistics Systems in Banks: Lithuanian Case Study. *Logistics*, *5*(3), 42.

[80] Van Greuning, H., & Bratanovic, S. B. (2020). *Analyzing banking risk: a framework for assessing corporate governance and risk management*. World Bank Publications.

[81] Verma, S., & Gustafsson, A. (2020). Investigating the emerging COVID-19 research trends in the field of business and management: A bibliometric analysis approach. *Journal of business research*, *118*, 253-261.

[82] Wong, P. K. (2022). *IT governance: a study of implementation, evolution and critical success factors* (Doctoral dissertation, Macquarie University).

[83] Yandri, R., Utama, D. N., & Zahra, A. (2019). Evaluation model for the implementation of information technology service management using fuzzy ITIL. *Procedia Computer Science*, *157*, 290-297.

[84] Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. *Continuity & Resilience Review*, *5*(1), 53-78.

[85] Yordanov, Y. (2022). Analysis of Methods for IT Service Management Processes Implementation in Higher Education Institutions. *Engineering 4.0 and the Internet of Everything*, 85.

[86] Zabolotniaia, M., Cheng, Z., Dorozhkin, E., & Lyzhin, A. (2020). Use of the LMS Moodle for an effective implementation of an innovative policy in higher educational institutions. *International Journal of Emerging Technologies in Learning*, *15*(13).