International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 1, Jan-Feb 2026
Available at wwwijsred.com
RESEARCH ARTICLE OPEN ACCESS

Integrating Zero Trust Security Model into Vendor Risk Management: Issues and Challenges

Olukayode Sorunke, CFE, CC, CySA+, CISA, CISM
Principal Consultant/ Senior Researcher
International Cyber Analytics Consulting Group, Arlington, Texas
Email: Osorun1@wgu.edu

Abstract

As organizations increasingly rely on third-party vendors for critical business operations, the traditional perimeter-based security approach has proven inadequate in mitigating evolving cyber threats. A breach of their third-party vendor could mean a breach of the entire enterprise. Hence, it is very imperative to ensure that the third-party vendor risks are properly identified and managed. A Zero Trust security Model has been identified as a strategic means of mitigating and managing third-party vendor risk.

This paper explores the integration of a Zero Trust security model into Vendor Risk Management (VRM) to strengthen organizational cyber resilience. Zero Trust, which operates on the principle of "never trust, always verify," mandates continuous authentication, strict access controls, and real-time monitoring, regardless of user location or device. This paper explores the integration of the Zero Trust architecture into Vendor Risk Management (VRM) frameworks, highlighting the benefits, implementation considerations, and the significant challenges organizations face in aligning the two paradigms. Key issues such as technological complexity, organizational resistance, scalability, and limited visibility into vendor environments are analyzed

Through focused panel discussion, case examples, and implementation strategies, the paper highlights key challenges—such as legacy system compatibility, cultural resistance, and increased complexity—and offers solutions for a phased, scalable deployment. By embedding Zero Trust principles into VRM, organizations can better safeguard sensitive data, reduce attack surfaces, and enhance overall third-party security posture in an increasingly interconnected digital ecosystem. The paper concludes with strategic recommendations for a phased, risk-based adoption of Zero Trust principles in VRM to strengthen supply chain security and overall cyber resilience.

Keywords: IT Outsourcing, Third-Party, Vendor Risk Management, Zero Security Trust Model,

1. Introduction

With the increasingly globalized and interconnected economy, it has become imperative for organizations to outsource some of their business operations to a third party with a view to focusing on the core business operations. In recent times, more businesses have moved their presence online, and companies have adopted cloud-based work; thus, it may be reasonable and economical to outsource some of these functions, such as application development, cloud services, network management, cybersecurity operations, data storage, and hosting, to external third-party vendors to manage on behalf of the client company. In the information technology industry, IT outsourcing is a common thing. It involves the practice of contracting IT services or functions to third-party vendors rather than managing them in-house.

While outsourcing has huge benefits for specialization, cost savings, scalability, and improved efficiency, it has also created a significant threat and vulnerability for businesses. The failure or breach by these third-party vendors can significantly impact a business entity's operational effectiveness and can further erode public confidence, trust, and reputation. Studies have shown

that outsourcing helps organizations reduce costs, access specialized expertise, and scale quickly, but it is prone to external dependencies, inherent risk, and vulnerabilities such as regulatory and compliance violations, cyber threats, and fraud threats.

Third-party relationships often involve access to privileged information like customer data and internal systems, making them potential entry points for cyberattacks. (Finio and Downie, 2024). According to a report by Gartner (ND), 40% of compliance leaders say that between 11% and 40% of their third parties are high-risk. As a result, organizations are now taking a greater interest in third-party risk management. Traditional cybersecurity models have proven inadequate in addressing these dynamic challenges, leading to the emergence of the zero Trust (ZT) security model-a paradigm shift towards a more proactive approach to risk management and trust assessment (Pigola et al, 2024). Unlike perimeter-based models, the Zero Trust model emphasizes the use of a dynamic, risk-adaptive approach for access authentication (Buck et al., 2021). It also relies on multi-factor authentication, identity management, real-time anomaly detection, endpoint security, and encryption to secure assets and minimize lateral movement (Rose et al., 2020; Teerakanok et al., 2021).

However, integrating these technologies poses challenges in implementation and management. (Pigola and Meirelles, 2025). The management challenges of Zero Trust model implementation across diverse organizational contexts, particularly the lack of universally accepted management criteria, remain largely unaddressed (Uttecht, 2020). Therefore, the goal of this paper is to see how this can be addressed through a systematic literature review of previous studies and the adoption of a focus group panel discussion. With all intent and purpose, the aim of this current study is to provide a nuanced understanding of how Zero Trust is being adopted across industries, its practical use cases, and the hurdles faced during implementation (Astillo et al., 2021).

2. Conceptual Clarification and Review of Literature

Concept of Third-Party Risk Management

Third-party risk exposure begins when a business entity or organization gives an external party or vendor access to their infrastructure, facilities, network, data, or information without exercising proper control and risk monitoring of the access granted. Where the third-party vendor system is compromised, the client company may experience devastating financial, reputational, regulatory, operational, and strategic consequences. Third-party failures have caused catastrophes in healthcare, banking, hospitality, manufacturing, retail, and the public sector, and they continue to make front-page news, especially cybersecurity-related failures. Third parties are often the weakest link, making them much easier to target by cybercriminals. In fact, 63% of all cyberattacks could be traced either directly or indirectly to third parties (PWC,2018).

Third-party risk management (TPRM), also known as vendor risk management, is a comprehensive approach to addressing inherent vulnerabilities associated with various third-party engagements and relationships. It involves identifying, assessing, and mitigating risks associated with outsourcing tasks or business operations to third-party vendors or service providers. ISACA defines third-party risk management (TPRM) as “the process of analyzing and controlling risks presented to your company, your data, your operations, and your finances by parties other than your company”. Managing third-party risk in today’s dynamic and volatile business environment is far from straightforward. It involves the development and adoption of a holistic and strategic policy. In recent times, we have seen massive supply chain disruptions, data breaches, enforcement actions, and a stunning series of cyberattacks emanating from poor management of third-party risk. An effective third-party risk management can help organizations secure their operations in an interconnected outsourced environment; it can also protect organizations from inherent risks and help build stronger and more resilient partnerships.

Third-party risk management focuses on identifying, assessing, and mitigating risks associated with third-party service providers. It encompasses risk classification, due diligence, performance monitoring, and incident response planning (Renaud & Goucher,

2021). Third-party risk management involves developing a comprehensive strategy for addressing inherent risks throughout the vendor relationship lifecycle. It normally involves four phases: risk identification, assessment, response, monitoring, and reporting.

Concept Of Zero Trust Model

The Zero Trust model, popularized by Forrester Research and later formalized by NIST (SP 800-207), is based on the core idea that no entity—internal or external—should be trusted by default. The concept of Zero Trust is a security model that operates on the principle of "never trust, always verify", ensuring that every user and device is authenticated and authorized before accessing a resource, regardless of their location. "Zero Trust is a principle-based model designed within a cybersecurity strategy that enforces a data-centric approach to continuously treat everything as an unknown-whether a human or a machine, to ensure trustworthy behavior" (Community Paper 2022).

To put it succinctly, every access request is fully authenticated, authorized, and encrypted before granting access. It is a security strategy that is based on the principle of continuous verification and least-privilege access over implicit trust, explicit, in other words, instead of believing that everything behind the organization's firewall is safe, the zero-trust model assumes breach and verifies each request as if it originated from an uncontrolled network. Unlike traditional perimeter-based security models, which assume trust once an entity gains access to the network, zero trust fundamentally challenges this notion by treating every interaction as untrustworthy until explicitly verified. (Kindervag,2011; Kudrati and Pillai, 2022; Pigola and Meirelles,2025

Zero Trust focuses on protecting resources at a granular level, employing technologies like multi-factor authentication, identity and access management, and encryption. It enforces the least privilege of access controls, minimizing unauthorized access and potential damages from breaches. (Edwards, 2023). This granular security approach also helps address cybersecurity risks posed by remote workers, hybrid cloud services, personally owned devices, and other elements of today's corporate network (Lindemulder & Kosinski, 2024).

In recent years, scholars and IT professionals have posited that the best approach to better manage an organization's risk exposure is to trust nobody. Zero Trust model, as the name suggests, postulates that organizations should take a holistic approach of "trust-no-one, whether someone is accessing the organization's resources, applications, or network, either from inside or outside the organization. It is about verifying everything, every user, every device, every time that someone tries to access the organization's network. Zero Trust is about constant verification that each person is where they should be and accessing only what they need and are authorized to touch, at every moment they are accessing the organization's network or application. (Uttreja, 2024).

The Zero Trust architecture assumes no inherent trust in users or systems, whether inside or outside the network perimeter. Key principles include continuous authentication, least-privilege access, micro-segmentation, and real-time monitoring (Rose et al., 2020). Zero Trust model, although not a new concept, has become more prominent in the IT environment because of the massive shift to remote work as well as the growing popularity of the "bring your own device" (BYOD) practices that emphasize the need for organizations to secure their workforce and digital workplaces. Zero Trust frameworks depend on continuous verification, strict identity management, and micro-segmentation to minimize trust (Kindervag, 2010). NIST Special Publication 800-207 provides a conceptual framework for zero trust. While the publication did not provide a comprehensive "fit it all" solution, nonetheless, the conceptual framework can be used as a tool to understand and develop a strategic Zero Trust policy for an organization.

The Need for Zero Trust in Vendor Risk Management

Vendor ecosystems often span multiple geographies, systems, and regulatory jurisdictions. Vendors may require access to sensitive data or privileged network zones, making them attractive targets for cybercriminals. Traditional security models, which

rely on fixed perimeters and implicit trust, are insufficient in such environments.
Benefits of integrating Zero Trust into VRM include:

- Enhanced control over vendor access and activity
- Reduction in the attack surface via access minimization
- Real-time detection of anomalies and threats originating from third-party connections
- Improved compliance with cybersecurity and data protection regulations

3. Materials and Methods

This study employs a comprehensive mixed-methods approach, integrating both Systematic Review of Literature (SLR) and qualitative focus group research methods to investigate the issues and challenges surrounding integrating the Zero Trust Model into third-party/vendor risk management. The design of the research is built on a systematic review of previous studies, frameworks, industry reports, and white papers on the Zero Trust Model using the PRISMA methodology to ensure transparency, completeness, replicability, and robustness of the study.
The research design also adopts a focus-group approach to collect relevant information from IT managers and cybersecurity professionals to support or disagree with findings from previous studies. The focus group consists of twenty IT managers and Cybersecurity professionals drawn from various organizations here in the United States, who have recently implemented or are planning to integrate the Zero Trust Model into their respective organizations' vendor risk management. By exploring the experiences and perspectives of IT professionals, cybersecurity experts, and other relevant stakeholders, this study was able to provide valuable insights into the current state of Zero Trust in vendor risk management, its impact on organizational security, cost and resource requirements, its potential benefits, operational efficiency, and challenges during implementation.

4. Results and Discussion

The systematic review of previous studies on zero trust implementation and integration into vendor risk management shows that organizations encountered numerous challenges. One of the most prominent challenges encountered is the issue of Legacy Systems Integration and compatibility, as highlighted by members of the focus group panel. Numerous organizations depend on traditional legacy equipment, which depends on network location as its main security admission standard, rather than authenticating devices or users by their identity or security status. Implementing Zero Trust requires significant upgrades to infrastructure, including identity and access management (IAM) systems, endpoint detection, and micro-segmentation technologies. Many organizations lack the technical maturity or budget to deploy and integrate these tools across their vendor ecosystems (CISA, 2021). Zero Trust demands that companies must continuously check user and device authenticity throughout their network, regardless of location. (Amomo,2025). Managing continuous authentication, access controls, and monitoring for hundreds or thousands of vendors can strain IT and security teams. Automating access provisioning and revocation is critical but often underdeveloped in existing systems (Forrester, 2020).
Third-party vendors vary widely in their security capabilities. Smaller vendors may not support advanced authentication protocols or real-time monitoring, creating gaps in the Zero Trust framework (ENISA, 2023). Vendors often operate outside the organization's direct control, making it difficult to enforce Zero Trust policies uniformly. Shadow IT and indirect access paths (e.g., through subcontractors) further complicate the security landscape (ISACA, 2023). Implementing the Zero Trust model requires seamless integration of various security tools, technologies, and processes. Organizations may encounter compatibility issues between existing infrastructure and new Zero Trust solutions, complicating the deployment process (Choudhury et al., 2020). Interconnecting various components while ensuring seamless functionality is pivotal to realizing the holistic benefit of Zero Trust (Ghasemshirazi et al, 2023). Also, it is very instructive to note that several legacy systems need long operational lifespans, so changing them to work with Zero Trust principles often proves unattainable. The process of retrofitting systems typically demands

infrastructure re-engineering that leads to disruptions along with service downtime. Roose (2021) highlights this as a significant barrier, noting that retrofitting older systems can be technically challenging and costly. Therefore, it is imperative for organizations to deploy various transition plans that enable legacy and Zero Trust systems to work alongside each other until complete integration becomes possible (Morris & Taylor, 2020).

Another major challenge identified by the focus group panel is the problem of organizational culture toward change. Transitioning to Zero Trust involves a fundamental shift in mindset—from trusting known actors to validating every transaction. Internal stakeholders and vendors alike may resist the increased scrutiny, viewing it as disruptive or bureaucratic (PWC, 2022). Organizational resistance to change and cultural misalignment with Zero Trust principles are well supported by previous studies, as highlighted by Zyoud and Lebai Lutfi (2024). Organizational support and acceptance are indeed critical factors that can make or mar the successful integration of the Zero Trust model into vendor risk management. Studies have shown that employees may resist changes to their established workflows, particularly if they do not understand the rationale behind the transition (Roose, 2021). Where employees and stakeholders have been accustomed to traditional security measures, resistance to adopting new practices, particularly if they perceive Zero Trust as overly restrictive, is very imminent (Zscaler, 2020). Therefore, successful implementation will require commitment from leadership to foster a culture of security awareness and compliance. Organizations should actively involve stakeholders in the Zero Trust adoption process to foster understanding and acceptance of new security measures. (Ajayi,2025). Lack of proper training, together with inadequate leadership communication, creates obstacles to slow down Zero Trust adoption and increases difficulties (Miller & Kline, 2019).

Financial Considerations are another key challenge identified as an obstacle to successful zero-trust model integration into vendor risk management. According to the focus group panelist, implementing a zero-trust model in vendor risk management comes with a substantial cost, as the Zero Trust Model implementation is known for its expensive initial investment, the upfront investment may deter organizations from pursuing this security model. Organizations may face high initial costs associated with upgrading legacy systems, implementing new technologies, and training staff (Zscaler, 2020). Zero Trust, which advocates "never trust, always verify," is increasingly seen as a robust framework for securing vendor interactions. Yet, its adoption poses significant financial implications, especially for small to mid-sized enterprises (SMEs) with limited cybersecurity budgets. According to Wannere (2025), some SMEs reported resource constraints, with initial deployment costs being a significant barrier. Initial costs often include infrastructure upgrades, new identity and access management (IAM) systems, micro-segmentation tools, and endpoint detection and response (EDR) platforms. These expenditures can be prohibitively high for organizations lacking pre-existing architecture aligned with ZTM (Forrester, 2021).

Recommended Best Practices and Strategies for Integrating the Zero Trust Model

While challenges such as integration with legacy systems, resistance to new changes, and cost constraints persist, organizations can mitigate these issues through phased implementation strategies. According to the findings from the focus group, the integration of the zero-trust model into vendor risk management can start by deploying zero-trust components in the high-risk areas of vendor management before expanding to cover the entire vendor management process. By embarking on phase implementation, the initial cost implication can be spread over phases. Implementing the Zero Trust Model in phases allows organizations to spread out costs. Initial efforts can focus on high-risk vendors or critical systems, gradually expanding to the broader ecosystem (NIST SP 800-207, 2020).

Apply Zero Trust controls proportionally. High-risk vendors (e.g., those with access to sensitive systems) should be prioritized for advanced controls, while low-risk vendors may require lighter oversight. The

organization would also need to enforce strong multi-factor authentication (MFA), role-based access control (RBAC), and just-in-time (JIT) access for all vendor users.

Conduct a VRM Maturity Assessment by evaluating the current state of vendor risk management and identifying gaps in access control, monitoring, and visibility. Use maturity models to set realistic goals. The use of automation for vendor onboarding, access reviews, and anomaly detection. AI-powered analytics can enhance visibility and responsiveness. It is also imperative that organizations that implement a zero-trust model in vendor risk management collaborate and communicate clearly. Work with vendors to improve their security posture. Include Zero Trust requirements in contracts and service-level agreements (SLAs), and offer training or tools to support compliance.

Lastly, the organizations should dedicate financial resources towards developing training and education programs to educate all the stakeholders about the need to embrace new cultural requirements. As pointed out by Ajayi (2024), the best practices for integrating a zero-trust model into vendor risk management include fostering a culture of security, providing adequate training, and adopting an incremental approach to implementation.

5. Conclusion, Limitations, and Future Directions

Integrating the Zero Trust model into Vendor Risk Management is no longer optional—it is essential for safeguarding digital supply chains against sophisticated cyber threats. The framework creates a strong mechanism to protect critical data, which can ultimately prevent attackers who may penetrate the internal network from gaining effortless access to additional resources or from elevating their privileges. While the journey is complex and fraught with challenges, a well-executed integration strategy can significantly enhance visibility, control, and resilience. Organizations must adopt a risk-based, phased approach and invest in the right technologies and partnerships to realize the full benefits of Zero Trust in the extended enterprise. While the Zero Trust Model offers a robust pathway to securing vendor ecosystems, its integration into Vendor Risk Management requires careful financial planning. Direct costs, operational burdens, and scalability concerns must be balanced against potential savings from breach mitigation and improved compliance. Organizations are encouraged to adopt a risk-based and phased approach, leveraging emerging technologies and industry incentives to optimize their financial outlay while achieving robust security outcomes.

While this study provides valuable insights into the challenges of integrating the zero-trust model into Vendor risk management, it is imperative to acknowledge certain limitations. The deployment of Zero Trust frameworks faces multiple implementation difficulties because the

needs to work with existing systems, scale properly, and enhance user interactions. The findings from this current study point out the requirement for additional empirical studies that will critically analyze the extended cost-effectiveness of implementing Zero Trust solutions into vendor risk management. The sample size of 20 experts on the focus group panel may limit the generalizability across different industries, regions, and organizational sizes. Future research should include broader sampling to improve the framework's applicability to sectors such as critical infrastructure, finance, supply chain, and healthcare.

Reference

Ajayi, O (2024): overcoming ZTA Adoption Challenges: A Framework for Integrating ZERO Trust Principles into Existing Network Infrastructure. International Journal of Modern Science and Research, Volume 2, Issue 10, ISSN No. 2584- 2706.

Astillo P, Choudhary G, Duguma D, Kim J, You I. TrMAps: Trust Management in Specification-Based Misbehavior Detection System for IMD-Enabled Artificial Pancreas System. IEEE J Biomed Health Inform 2021; 25:3763 75. https://doi.org/10.1109/JBHI.2021.3063173.

Buck, C., Olenberger, C., Schweizer, A., Völter, F. and Eymann, T. (2021). "Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust", Computers and Security, Vol. 110, p. 102436, Doi: 10.1016/j.cose.2021.102436.

CISA. (2021). Zero Trust Maturity Model. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov

Community Paper (2022): The Zero Trust Model in Cybersecurity: Toward Understanding and Deployment. Retrieved from www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf

Choudhury, P., Debnath, N., & Barua, S. (2020). Zero Trust Security Architecture: A Review. International Journal of Computer Applications, 176(17), 25–30. doi:10.5120/ijca2020920620.

Edward, M (2023). How ISO27001 can help Organizations Implement a zero-trust security Model. Retrieved on 06/26/2025 from www.isms.online/knoledge/iso-27001-and implementing-a zero-trust-security-model/

ENISA. (2023). Supply Chain Security for ICT Products and Services. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Finio. M and Downie. A (2024). What is third-party risk management (TPRM) ? retrieved on 06/25/2025 from www.ibm.com/think/topics/What is Third-Party Risk Management (TPRM)? | IBM

Forrester (2020). The Forrester Wave™: Zero Trust Extended Ecosystem Platform Providers, Q4 2020.

Forrester (2021). The Total Economic Impact of Zero Trust Extended Ecosystem. Forrester Research.

Fusion (2021): Third-Party Risk Management 101 retrieved on 06/25/2026 from Third-Party Risk Management 101 - Fusion

Gartner (ND): Build an Efficient, Effective third-party risk management program. Retrieved on 06/25/2025 from www.gartner.com/en/legal-compliance/topic/ Third-Party Risk Management (TPRM): A Complete Guide

Ghasemshirazi. S Shirvani, G, and Alipour, M (2023): Zero Trust: Applications, Challenges, and Opportunities. Retrieved from https://www.researchgate.net/publication/373753509_Zero_Trust_Applications_Challenges_and_Opportunities.

IBM (2023). Cost of a Data Breach Report. IBM Security. https://www.ibm.com/reports/data-breach

ISACA. (2023). State of Cybersecurity 2023: Global Update on Workforce Efforts and Threat Landscape. https://www.isaca.org

Kindervag, J. (2010). "Build security into your network's DNA: the zero trust network architecture", Forrester Research, Vol. 27, pp. 1-16.

Kudrati, A. & Pillai, B.A. (2022). Zero Trust Journey across the Digital Estate, 1st ed. CRC Press, Boca Raton, Doi: 10.1201/9781003225096

Lindemulder, G, & Kosinski, M (2024). What is Zero Trust? Retrieved on 06/26/2025 from www.ibm.com/think/topics/zero-trust What Is Zero Trust? | IBM

Morris, A., & Taylor, F. (2020). Integrating zero trust with legacy systems: Challenges and strategies. International Journal of Cybersecurity, 15(3), 90–102.

NIST. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-207/final

Pigola, A, & Meirelles, F (2025). Zero Trust in Cybersecurity: Managing Critical Challenges for Effective Implementation. Journal of Systems and Information Technology, April 2025. Doi.10.1108/jsit-08-2024-0326.

Pigola, A., Meirelles, F., Da Costa, P., & Porto, G. (2024). "Trust in information security technology: an intellectual property analysis", World Patent Information, Vol. 78, p. 102281, Doi: 10.1016/j.wpi.2024.102281.

PWC. (2022). Cybersecurity Outlook 2022. PricewaterhouseCoopers. https://www.pwc.com

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020). Zero Trust Architecture, National Institute of Standards and Technology, Doi: 10.6028/NIST.SP.800-207, available at: www.nist.gov/ publications/zero-trust-architecture (accessed 30 June 2025)

Roose, K. (2021). Why Zero Trust Is a Game Changer in Cybersecurity. Harvard Business Review. Retrieved from the HBR website.

Scott R (2022). Planning for zero Trust Architecture: A planning Guide for federal Administrators. Retrieved on 06/26/2025 from https://doi.org/10.6028/NIST.CSWP.20

Uttecht, K.D. (2020). "Zero trust (ZT) concepts for federal government architectures", No. FA8702-15-

D0001, Massachusetts Institute of Technology, Lincoln Laboratory, Lexington, MA, pp. 1–58.
Uttreja, N (2024). Zero Trust Architecture: Building a Resilient Cybersecurity Framework with Key Technologies and Strategies. Retrieved on 06/26/2025 from www.isc2.org/ Zero Trust Architecture: Building a Resilient Cybersecurity Framework with Key Technologies and Strategies
Wannere, K (2025). Exploring the Implementation and Challenges of Zero Trust Security Models in Modern Network Environments. International Journal of Engineering Research & Technology (IJERT) Vol.. 14 Issue 05, Retrieved from exploring-the-implementation-and-challenges-of-zero-trust-security-models-in-modern-network-environments-IJERTV14IS050146.pdf
Zscaler. (2020). Zero Trust Security: A Guide to Protecting Your Digital Assets. Retrieved from the Zscaler website.
Zyoud, B. & Lebai Lutfi, S. (2024). "The role of information security culture in zero trust adoption: insights from UAE organizations", IEEE Access, Vol. 12, pp. 72420–72444, Doi: 10.1109.

