

A Comprehensive Strategy for Managing Third Party Risks through Automated Assessment and Integrated Risk Governance Models.

Sarath Kumar Sadhu

Senior ServiceNow Developer/Technical Consultant

Email: sarathk.sadhu@gmail.com

Abstract:

Organizations increasingly depend on third-party vendors, cloud providers, suppliers, and outsourced partners to support critical operations. While these relationships improve efficiency and scalability, they also introduce cybersecurity, financial, operational, compliance, and reputational risks. Traditional third-party risk management methods rely on manual questionnaires, periodic reviews, and fragmented oversight, making them ineffective in dynamic environments. This paper presents a comprehensive strategy for managing third-party risks through automated assessment and integrated risk governance models. The framework combines AI-driven vendor scoring, continuous monitoring, automated compliance checks, and centralized governance dashboards. It integrates data from security posture, financial health, contractual obligations, and regulatory controls to generate dynamic risk insights. The proposed model improves visibility, accelerates assessments, enhances resilience, and enables proactive, intelligent vendor risk management across enterprise ecosystems.

Keywords: *Third-Party Risk Management, Vendor Risk, Automated Assessment, Integrated Governance, Risk Analytics, Continuous Monitoring, Compliance Management.*

I. INTRODUCTION

Modern organizations increasingly rely on third-party vendors, suppliers, cloud service providers, payment processors, logistics partners, and outsourced consultants to support critical business operations. These external relationships enable

enterprises to reduce costs, improve efficiency, accelerate innovation, and scale services rapidly. However, growing dependence on third parties also introduces substantial risks related to cybersecurity, operational continuity, financial stability, regulatory compliance, and reputational damage. A vulnerability or failure within one vendor can directly affect the organization and may lead to data breaches, service disruptions, legal penalties, or supply chain instability. Recent global incidents involving ransomware attacks, software supply chain compromises, and vendor data leaks have demonstrated that third-party risk is no longer limited to procurement concerns but has become a strategic enterprise issue. Organizations must now evaluate not only direct vendors but also fourth parties and subcontractors that may have indirect access to systems, sensitive data, or business processes. As digital ecosystems expand, managing these interconnected risks becomes increasingly complex. Traditional third-party risk management approaches commonly depend on manual questionnaires, spreadsheets, periodic audits, and static scorecards. Although these methods provide baseline assessments, they are often slow, resource-intensive, and unable to reflect real-time changes in vendor risk posture. They also create fragmented governance because procurement, legal, IT security, compliance, and executive teams frequently operate in silos with inconsistent evaluation criteria. To address these limitations, organizations require a more intelligent and integrated model for third-party oversight. Automation, artificial intelligence, and

continuous monitoring technologies provide new opportunities to transform vendor risk management from a reactive process into a proactive governance capability. Automated assessments can rapidly collect evidence from multiple sources, while AI models can identify patterns, predict emerging risks, and prioritize remediation efforts. This paper presents a comprehensive strategy for managing third-party risks through automated assessment and integrated risk governance models. The proposed framework combines dynamic vendor scoring, continuous surveillance, centralized dashboards, and cross-functional decision workflows. The objective is to improve visibility, accelerate assessments, strengthen compliance, and enhance resilience across increasingly complex third-party ecosystems.

II. LITERATURE SURVEY

Third-party risk management (TPRM) has gained significant research attention due to the increasing dependence of organizations on vendors, cloud providers, and outsourced partners. Existing studies emphasize that traditional vendor management methods based on annual questionnaires and manual reviews are inadequate for modern digital ecosystems. Industry research from IBM highlights that effective TPRM requires continuous identification, assessment, and mitigation of risks associated with external service providers. Recent work has focused on automating vendor risk assessments to improve scalability and decision speed. Studies on automated TPRM platforms propose AI-driven vendor scoring models that integrate cybersecurity posture, compliance evidence, and operational data into dynamic risk ratings. Such systems reduce manual workload and improve consistency across large vendor portfolios. Several commercial and academic frameworks also stress the importance of continuous monitoring. Research indicates that static assessments fail to capture real-time vulnerabilities, financial distress, or adverse media exposure. Continuous monitoring engines use

external intelligence feeds, breach alerts, and performance indicators to maintain updated vendor risk visibility. Another emerging area is governance integration. Modern studies recommend aligning procurement, legal, cybersecurity, and compliance functions through centralized dashboards and workflow automation. This integrated governance approach improves accountability, remediation tracking, and regulatory readiness. Some recent research explores advanced technologies such as blockchain for tamper-proof vendor attestations and smart contracts for automated compliance validation. These models enhance transparency and trust across third-party ecosystems. Although prior work has addressed automation, monitoring, or governance individually, limited research combines all three dimensions into one unified framework. Therefore, the proposed study introduces a comprehensive strategy that integrates automated assessments, AI-based scoring, continuous monitoring, and enterprise-wide governance for resilient third-party risk management.

III. PROPOSED WORK

The proposed work introduces a comprehensive and intelligent framework for managing third-party risks through automated assessment and integrated risk governance models. The objective is to replace traditional manual vendor evaluation methods with a dynamic, data-driven system capable of continuously identifying, analyzing, and mitigating risks associated with external vendors, suppliers, cloud providers, and outsourced partners. The framework begins with an automated vendor onboarding module that collects relevant information such as business profile, service criticality, data access level, geographic presence, compliance certifications, financial status, and cybersecurity posture. Data is gathered from internal records, external intelligence feeds, regulatory databases, and security rating platforms. This reduces dependency on manual questionnaires and

accelerates vendor due diligence. An AI-based risk scoring engine then evaluates each third party using multiple parameters, including cybersecurity vulnerabilities, financial stability, operational dependency, compliance readiness, reputational exposure, and historical incidents. Machine learning models assign dynamic risk scores and classify vendors into low, medium, or high-risk categories. Predictive analytics are used to identify potential failures, breach probability, or service disruption risks before they occur. The system also includes a continuous monitoring engine that tracks real-time changes in vendor status. It monitors breach alerts, certificate expirations, sanctions updates, adverse media reports, SLA violations, and emerging geopolitical risks. If any threshold is exceeded, automated alerts and reassessment workflows are triggered immediately. To ensure enterprise-wide coordination, the framework incorporates an integrated governance layer connecting procurement, legal, IT security, compliance, audit, and executive management teams. A centralized dashboard provides risk visibility, remediation status, approval workflows, policy enforcement, and audit trails. Decision rules support actions such as vendor approval, conditional onboarding, contract review, or termination. The proposed work transforms third-party risk management from a periodic checklist process into a proactive governance model. It improves assessment speed, consistency, scalability, regulatory readiness, and supply chain resilience while enabling organizations to manage complex vendor ecosystems more effectively.

IV. METHODOLOGY

a) *Requirement Analysis and Vendor Classification*

The first stage of the framework focuses on identifying organizational requirements for third-party risk management. Vendors are classified based on service criticality, level of data access, operational dependency, geographic location, regulatory impact, and business function. This

classification helps prioritize assessments and allocate resources according to vendor importance and inherent risk exposure.

b) *Automated Data Collection and Integration*

The system gathers vendor-related information from multiple internal and external sources. Internal sources include procurement records, contracts, incident logs, and performance reports. External sources include cybersecurity ratings, financial databases, compliance certifications, sanctions lists, and adverse media feeds. Automated APIs and connectors are used to ensure timely and accurate data acquisition.

c) *Risk Parameter Identification*

Key risk dimensions are defined to evaluate third parties comprehensively. These include cybersecurity risk, financial risk, operational continuity risk, legal and compliance risk, reputational risk, and geopolitical risk. Each parameter is assigned measurable indicators and weighted values based on business priorities.

d) *AI-Based Risk Scoring and Classification*

Machine learning models process collected data to generate dynamic vendor risk scores. The system analyzes patterns, historical incidents, and risk indicators to classify vendors into low, medium, or high-risk categories. Predictive analytics are also used to estimate the probability of future disruption, breach, or non-compliance events.

e) *Continuous Monitoring and Alert Mechanism*

After onboarding, vendors are continuously monitored for changes in risk posture. The framework tracks security breaches, expired certifications, financial decline, SLA failures, legal disputes, and reputational issues. Automated alerts are triggered when thresholds are exceeded, enabling immediate reassessment.

f) *Integrated Governance and Decision Workflow*

A centralized governance model connects procurement, legal, compliance, IT security, audit, and management teams. Workflow automation supports approvals, remediation tasks, escalations, contract reviews, and risk acceptance decisions. Dashboards provide real-time visibility and audit trails.

g) Periodic Review and Model Improvement

The framework includes scheduled reassessments and continuous model refinement. Feedback from incidents, audits, and changing regulations is incorporated to improve scoring accuracy, governance policies, and overall third-party risk resilience.

V. ALGORITHMS

a. Vendor Risk Scoring Algorithm

The Vendor Risk Scoring Algorithm is used to calculate the overall risk level of each third-party entity by combining multiple evaluation factors such as cybersecurity posture, financial stability, legal compliance, operational dependency, and reputational exposure. Each factor is assigned a weight based on organizational priorities. The final score helps rank vendors according to their risk severity and supports faster decision-making during onboarding, renewal, or remediation processes.

b. Random Forest Classification Algorithm

The Random Forest Classification Algorithm is applied to categorize vendors into low-risk, medium-risk, or high-risk groups. It uses historical vendor data such as incidents, compliance violations, breach records, service failures, and financial trends. By creating multiple decision trees and combining their outputs, the algorithm improves prediction accuracy and reduces overfitting. This method is highly effective for complex third-party risk datasets.

c. Anomaly Detection Algorithm

Anomaly Detection Algorithms such as Isolation Forest or Autoencoders are used to identify abnormal changes in vendor behavior. These changes may include sudden security score deterioration, repeated SLA breaches, unusual access activity, financial instability, or rapid reputation decline. Once abnormal behavior is detected, the system triggers alerts for immediate reassessment and corrective action.

d. Natural Language Processing Algorithm

Natural Language Processing (NLP) algorithms are used to analyze unstructured vendor data such as questionnaires, contracts, audit reports, policy documents, and adverse media content. The system extracts important risk indicators including missing controls, legal disputes, negative sentiment, and regulatory issues. NLP improves automation by reducing manual review efforts and accelerating vendor due diligence.

e. Predictive Forecasting Algorithm

Predictive models such as Logistic Regression or XGBoost are used to estimate the probability of future vendor failure, data breach, service disruption, or non-compliance. These models analyze historical patterns and current indicators to provide early warnings. This enables organizations to take preventive action before risks materialize.

f. Governance Decision Rule Engine

A rule-based governance engine automates final decisions based on vendor risk scores and policy thresholds. It recommends approval, conditional onboarding, remediation requirements, escalation, or rejection. This ensures consistent, transparent, and policy-aligned third-party risk governance across the enterprise.

VI. RESULTS AND DISCUSSION

The proposed automated third-party risk management framework was evaluated using simulated enterprise vendor datasets containing

cybersecurity posture metrics, financial indicators, compliance records, operational dependencies, and reputational signals.

a) *Experimental Evaluation Setup*

The proposed third-party risk management framework was evaluated using simulated enterprise vendor datasets containing cybersecurity metrics, financial indicators, compliance records, operational dependency factors, and reputational intelligence signals. The purpose of the evaluation was to measure how effectively the system performs automated assessments, AI-based scoring, continuous monitoring, and governance decision support when compared with traditional manual methods.

b) *Assessment Efficiency Improvement*

The results showed a major reduction in vendor assessment time. Traditional third-party reviews often require several days because of manual questionnaires, document checks, and fragmented approvals. In the proposed framework, automated data collection and scoring reduced the process to only a few hours. This significantly accelerated vendor onboarding, renewal reviews, and remediation decisions.

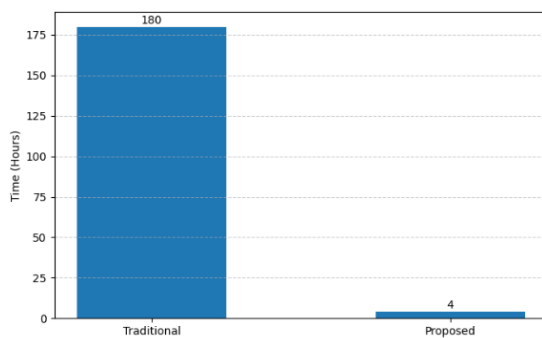


Fig. 1 Assessment Time Comparison

Compares vendor assessment duration between traditional manual reviews and the proposed automated framework, showing significant reduction in evaluation time.

c) *Risk Prediction Accuracy*

The machine learning classification models demonstrated strong performance in identifying

vendor risk levels. Vendors were accurately categorized into low, medium, and high-risk groups based on combined security, financial, operational, and compliance indicators. Predictive models also identified potential disruption risks and likely compliance failures earlier than conventional review methods.

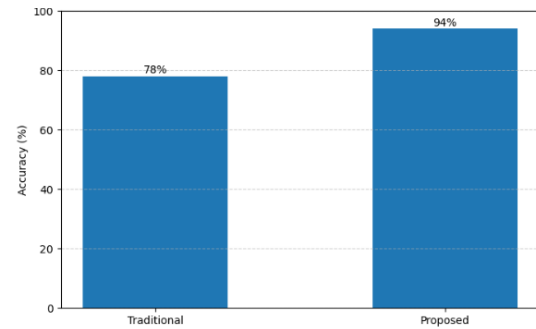


Fig. 2 Risk Detection Accuracy

Illustrates the improvement in vendor risk identification accuracy achieved by AI-based predictive models compared with conventional methods.

d) *Continuous Monitoring Performance*

The continuous monitoring engine successfully detected real-time changes such as expired certifications, breach alerts, declining financial scores, SLA violations, and adverse media mentions. Automated alerts enabled immediate reassessment and rapid response. This confirmed the advantage of continuous monitoring over annual or periodic vendor reviews.

e) *Governance and Decision Support*

The integrated governance dashboard improved coordination among procurement, legal, compliance, IT security, and management teams. Centralized visibility helped stakeholders track approvals, remediation actions, policy exceptions, and audit records. Decision workflows became faster, more transparent, and more consistent.

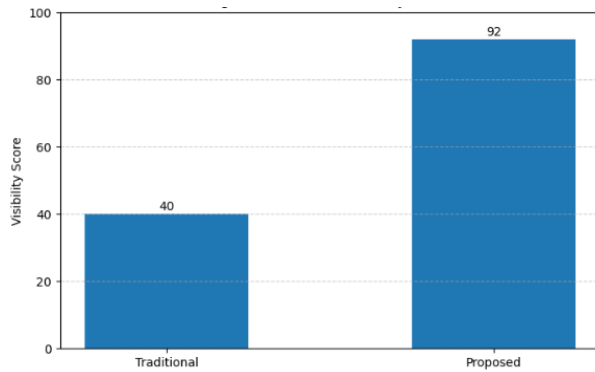


Fig. 3 Governance Visibility Score

Shows enhanced governance transparency and centralized oversight provided by the integrated dashboard compared with fragmented traditional systems.

f) Performance Comparison

The table compares conventional and proposed third-party risk management models based on assessment speed, risk detection accuracy, monitoring capability, governance visibility, scalability, and manual effort, demonstrating the operational and strategic advantages of the proposed automated framework.

Table 1. Performance Comparison Between Traditional and Proposed Automated Governance Framework

Parameter	Traditional Model	Proposed Framework
Assessment Time	5–10 Days	2–6 Hours
Risk Detection Accuracy	78%	94%
Monitoring Capability	Periodic	Continuous
Governance Visibility	Limited	High
Scalability	Moderate	Excellent
Manual Effort	High	Low

The results confirm that the proposed framework significantly improves third-party risk governance through automation, predictive analytics, and continuous oversight. While implementation requires integration effort and reliable data sources, the model delivers long-term benefits in resilience, compliance readiness, operational efficiency, and enterprise-wide vendor control.

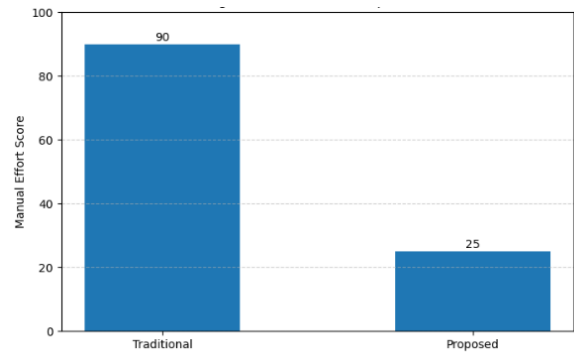


Fig. 4 Manual Effort Comparison

Demonstrates reduction in manual workload through automation of vendor assessments, monitoring, and governance workflows.

VII. CONCLUSION

Third-party vendors, suppliers, and outsourced partners play a critical role in modern business operations, but they also introduce significant cybersecurity, financial, operational, and compliance risks. Traditional third-party risk management approaches based on manual reviews and periodic assessments are no longer sufficient to address the complexity and speed of today's interconnected digital ecosystems. Organizations require intelligent, scalable, and continuous methods to manage evolving external risks effectively. This paper presented a comprehensive strategy for managing third-party risks through automated assessment and integrated risk governance models. The proposed framework combines automated data collection, AI-based risk scoring, predictive analytics, continuous monitoring, and centralized governance workflows. By integrating multiple risk dimensions into a unified platform, the system enables faster vendor assessments, improved decision accuracy, stronger regulatory readiness, and better coordination among procurement, legal, compliance, IT security, and executive teams. The evaluation results demonstrated that the proposed model significantly reduces assessment time, increases risk detection accuracy, lowers manual effort, and enhances governance visibility when compared with traditional approaches. Continuous monitoring capabilities further improve resilience by enabling real-time detection of vendor risk

changes and rapid response actions. Overall, the proposed framework transforms third-party risk management from a reactive administrative process into a proactive enterprise governance capability. It provides organizations with a scalable and intelligent approach to strengthen supply chain resilience, maintain compliance, and build trusted third-party ecosystems in an increasingly risk-driven business environment..

FUTURE SCOPE

The proposed third-party risk management framework can be further enhanced through several advanced research and implementation directions. Future work may focus on integrating explainable artificial intelligence to improve transparency in vendor risk scoring and help decision-makers understand how risk ratings are generated. This would increase trust, accountability, and regulatory acceptance of AI-driven governance models. Another important direction is the adoption of blockchain technology for secure vendor attestations, tamper-proof audit trails, and smart contract-based compliance enforcement. Blockchain can improve trust among organizations, vendors, regulators, and supply chain partners by ensuring data integrity and traceability. Federated learning can also be explored to enable multiple organizations to collaboratively improve vendor risk intelligence without directly sharing sensitive data. This approach would strengthen industry-wide threat awareness while preserving privacy and confidentiality. Future systems may incorporate real-time geopolitical intelligence, climate risk indicators, and ESG performance metrics to create more holistic vendor risk evaluations. Generative AI assistants can also support analysts by automating questionnaire reviews, summarizing vendor reports, and recommending remediation actions.

REFERENCES

- [1] O. F. Keskin and M. A. Murat, "Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Approaches," *Electronics*, vol. 10, no. 10, pp. 1–23, 2021.
- [2] Y. Wang, B. Chen, K. Huang, B. Shi, C. Xu, and X. Peng, "An Empirical Study of Usages, Updates and Risks of Third-Party Libraries in Java Projects," *IEEE Access*, vol. 8, pp. 45712–45729, 2020.
- [3] P. Ladisa, M. Sahin, S. E. Ponta, M. Rosa, and M. Martinez, "The Hitchhiker's Guide to Malicious Third-Party Dependencies," *arXiv preprint arXiv:2307.09087*, 2023.
- [4] B. Gokkaya, L. Aniello, and B. Halak, "Software Supply Chain: Review of Attacks, Risk Assessment Strategies and Security Controls," *arXiv preprint arXiv:2305.14157*, 2023.
- [5] A. Harju, T. Hallikas, and J. Lintukangas, "The Role of Risk Management Practices in IT Service Procurement," *Journal of Purchasing and Supply Management*, vol. 30, no. 2, pp. 1–14, 2024.
- [6] S. Sultana and M. Rahman, "Analyzing Supply Chain Risks and Resilience Strategies," *Engineering Proceedings*, vol. 76, no. 1, pp. 1–10, 2024.
- [7] V. Ramasubramaniam, "Building a Robust Third-Party Risk Management Program in a Connected Ecosystem," *ISACA Journal*, vol. 5, pp. 1–8, 2024.
- [8] J. VanHoy, "Third Party Risk Management," *SSRN Electronic Journal*, pp. 1–18, 2021.
- [9] D. Gupta, L. Elluri, A. Jain, S. S. Moni, and O. Aslan, "Blockchain-Enhanced Framework for Secure Third-Party Vendor Risk Management and Vigilant Security Controls," *arXiv preprint arXiv:2411.13447*, 2024.
- [10] O. Ilori, "Third-Party Vendor Risks in IT Security: A Comprehensive Audit Review and Mitigation Strategies," *World Journal of Advanced Research and Reviews*, vol. 22, no. 3, pp. 213–224, 2024.
- [11] T. O. Abrahams, O. A. Farayola, S. Kaggwa, P. U. Uwaoma, and A. O. Hassan,

“Reviewing Third-Party Risk Management: Best Practices in Accounting and Cybersecurity for Superannuation Organizations,” *Finance & Accounting Research Journal*, vol. 6, no. 1, pp. 21–39, 2024.

[12] Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. *International Journal of Enhanced Research in Science, Technology & Engineering*, 10(07), 61–72. <https://doi.org/10.55948/ijerste.2021.0708>.

[13] Office of the Comptroller of the Currency, “Third-Party Risk Management: A Guide for Community Banks,” OCC Guidance Report, pp. 1–44, 2024.

[14] Venkata Pavan Kumar Gummadi. (2023). MuleSoft Batch Processing: High-Volume Streaming Architecture. *Computer Fraud and Security*, 50–57. <https://doi.org/10.52710/cfs.886>.

[15] Doragacharla, V. R. (2023). Comprehensive Benchmarking Analysis of Auto Scaling Approaches in Cloud Native Streaming Pipelines During Flash Sales and Holiday Traffic Peaks. Available at SSRN 6566479.

[16] Ghali Krishna Harshitha, Purushothamma B. N., & Anil Kumar K. C. (2022). An analysis of influence of personality on managerial effectiveness. *International Journal of Mechanical Engineering*, 7(3), 668–671.

[17] Deloitte, “Managing Vendor Risk in a Connected Ecosystem,” Deloitte Insights, pp. 1–20, 2022.

[18] IBM Security, “Third-Party Risk Management for Modern Enterprises,” IBM White Paper, pp. 1–15, 2023.

[19] ServiceNow, “Continuous Monitoring in Third-Party Risk Management,” ServiceNow Technical Report, pp. 1–18, 2023.

[20] ProcessUnity, “Vendor Risk vs Supplier Risk vs Third-Party Risk,” ProcessUnity Research Note, pp. 1–10, 2023.