IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Securevendor: An Explainable Framework For Third-Party Risk Management

[1]Mr. Govind Nair, [2]Miss Trusha Suvarna, [3]Mr. Vaishak Menon, [4] Asst. Prof. Gauri Ansurkar

[1234] Keraleeya Samajam's Model College, Thakurli, Dombivli East, Mumbai, Maharashtra, India

Abstract: In today's interconnected digital ecosystem, organizations increasingly rely on third-party vendors and service providers for critical IT and business operations. However, these vendor relationships expose organizations to significant cybersecurity and compliance risks. Existing Third-Party Risk Management (TPRM) tools are often expensive, complex, and lack transparency in their scoring methodologies, making them impractical for small and mid-sized enterprises (SMEs).

This research proposes SecureVendor, a lightweight, transparent, and explainable TPRM framework that enables organizations to assess, monitor, and track vendor risks effectively. The proposed system introduces an explainable risk scoring mechanism, vendor remediation tracking, and continuous alerting features to address current gaps. The study uses both secondary (literature) and primary (public survey) research methods to evaluate the challenges and expectations of professionals in the cybersecurity and compliance domains. Findings from the survey validate the hypothesis that SMEs require more accessible, transparent, and action-oriented TPRM solutions.

Index Terms - Third-Party Risk Management, Vendor Risk, Cybersecurity, GRC, Compliance, Explainable Scoring, Remediation Tracking

I. INTRODUCTION

In recent years, the frequency of cybersecurity incidents originating from third-party vendors has significantly increased. Organizations today depend heavily on external vendors for IT infrastructure, software development, and data processing. While outsourcing enhances operational efficiency, it introduces considerable cybersecurity risks if vendors fail to maintain adequate controls.

Traditional vendor assessments are often conducted manually or through complex Governance, Risk, and Compliance (GRC) systems designed for large enterprises. This creates a gap where small and mid-sized organizations struggle to manage vendor risks effectively due to high costs and limited technical resources.

The goal of this research is to address these challenges through SecureVendor, an explainable and user-friendly TPRM framework that emphasizes transparency, simplicity, and continuous improvement.

II. PROBLEM STATEMENT

Despite the increasing importance of vendor cybersecurity management, existing Third-Party Risk Management tools primarily cater to large enterprises, offering limited flexibility and high costs for smaller organizations. Current tools often provide black-box risk scores with limited remediation tracking, leading to reduced vendor accountability and unclear decision-making.

There is, therefore, a pressing need for a transparent, explainable, and cost-effective framework that simplifies vendor assessments and enables organizations to continuously monitor and track vendor remediation activities.

III. RESEARCH HYPOTHESES

H1: Existing TPRM tools lack transparency and continuous monitoring, reducing their effectiveness among small and medium-sized enterprises.

H2: A lightweight and explainable TPRM tool with vendor remediation tracking and automated alerts will significantly improve vendor risk visibility and management efficiency.

H0: There is no significant difference between existing TPRM tools and the proposed approach in improving vendor risk visibility and control.

IV. OBJECTIVES OF THE STUDY

1. To evaluate the limitations and challenges faced by organizations using current TPRM tools.
2. To design and propose a transparent, lightweight TPRM framework (SecureVendor).
3. To integrate remediation tracking and continuous alerting features into the framework.
4. To validate the research hypothesis using a public survey of IT and cybersecurity professionals.

V. RESEARCH METHODOLOGY

1. Literature Survey: A comprehensive review of existing TPRM frameworks, academic publications, and industry reports was conducted using sources such as IEEE Xplore, SpringerLink, Gartner reports, and NIST publications. The focus was to identify challenges in existing tools, including complexity, high costs, and lack of transparency.
2. Public Survey: A structured questionnaire was distributed via Google Forms to professionals and students in the cybersecurity and IT domains. The survey aimed to gather insights on current practices in vendor risk management, challenges faced using existing tools, expectations from new frameworks, and interest in open, explainable, and automated TPRM solutions. Data collected was statistically analyzed to validate or refute the research hypotheses.
3. Proposed Framework: Based on literature and survey findings, a conceptual model named SecureVendor was proposed. It integrates explainable risk scoring, remediation workflows, and continuous alert notifications.

VI. LITERATURE SURVEY

Existing research and industry reports highlight multiple gaps in the current TPRM landscape. OneTrust and RSA Archer provide integrated TPRM solutions but remain expensive and complex for SMEs (Gartner, 2023). BitSight and Panorays focus on external risk ratings but lack explainability and vendor collaboration features (Panorays, 2024). NIST SP 800-161 Rev.1 and ISO/IEC 27036 emphasize supply chain risk management but do not provide practical implementation guidance for smaller organizations. Academic research suggests the need for AI-driven, transparent frameworks that promote continuous risk awareness.

From this review, it is evident that there exists a research and implementation gap between academic frameworks and practical, affordable TPRM systems — a gap that SecureVendor aims to bridge.

VII. PROPOSED SYSTEM – SECUREVENDOR

1. Overview: The proposed system, SecureVendor, is designed as a simple, transparent, and explainable TPRM framework that helps organizations assess and monitor vendor-related cybersecurity risks. It focuses on three key principles: transparency, accountability, and continuous improvement.
2. System Components:
- Vendor Management Module: Handles vendor registration and stores profile details.
- Risk Assessment Module: Uses structured questionnaires to evaluate vendor cybersecurity maturity.
- Risk Scoring Engine: Calculates a weighted score to categorize vendors as Low, Medium, or High risk.
- Remediation Tracking Module: Allows vendors to respond with corrective actions for identified risks.
- Monitoring and Alerts: Sends reminders and alerts for pending or recurring issues.
3. Workflow: The typical workflow includes: organization registers a vendor; vendor completes the assessment; the system generates a transparent risk score; vendor provides remediation updates; and the organization monitors progress via alerts and dashboards.
4. Expected Outcomes: Enhanced visibility into vendor risk posture; improved collaboration through transparent remediation tracking; and a cost-effective and accessible TPRM solution for SMEs.

VIII. RESULT AND ANALYSIS

A total of 31 participants took part in the survey, representing diverse IT and cybersecurity roles. The responses were analyzed quantitatively to understand the current awareness, adoption, and perception of Third-Party Risk Management (TPRM) practices in organizations.

Figure 1 shows the distribution of participant roles. These respondents represent professionals who commonly engage with vendor risk processes.

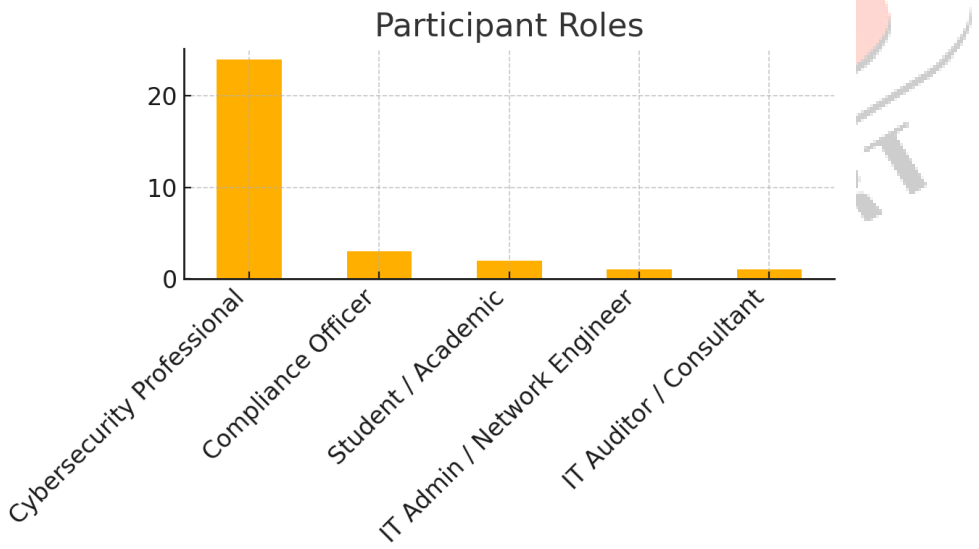

Figure 1: Distribution of Participant Roles

Figure 2 presents the years of experience of respondents, indicating a majority with 2–6 years in IT/security.

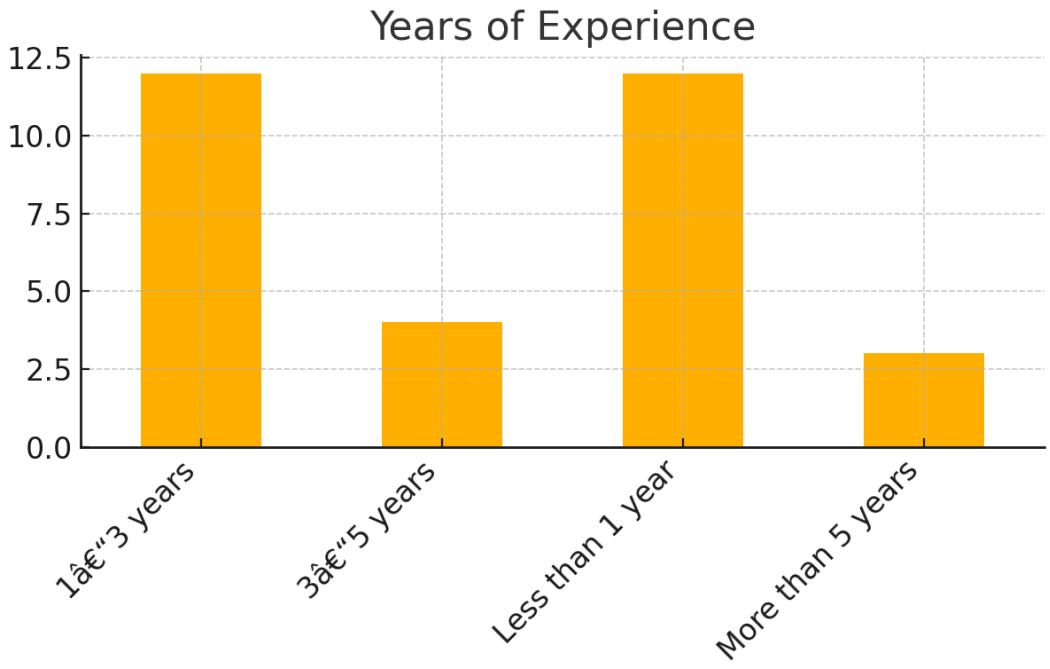

Figure 2: Years of Experience of Participants

Figure 3 describes the industry types of respondents, demonstrating a spread across IT, finance, healthcare, and others.

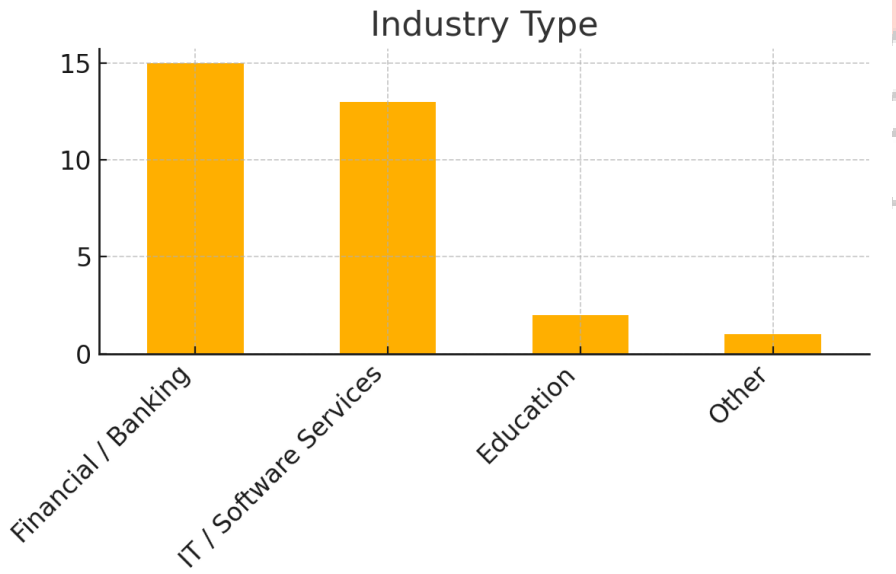

Figure 3: Industry Type of Respondents

Figure 4 summarizes awareness and adoption of TPRM practices within organizations. Over 80% were aware of TPRM, yet only 55% reported formal adoption.

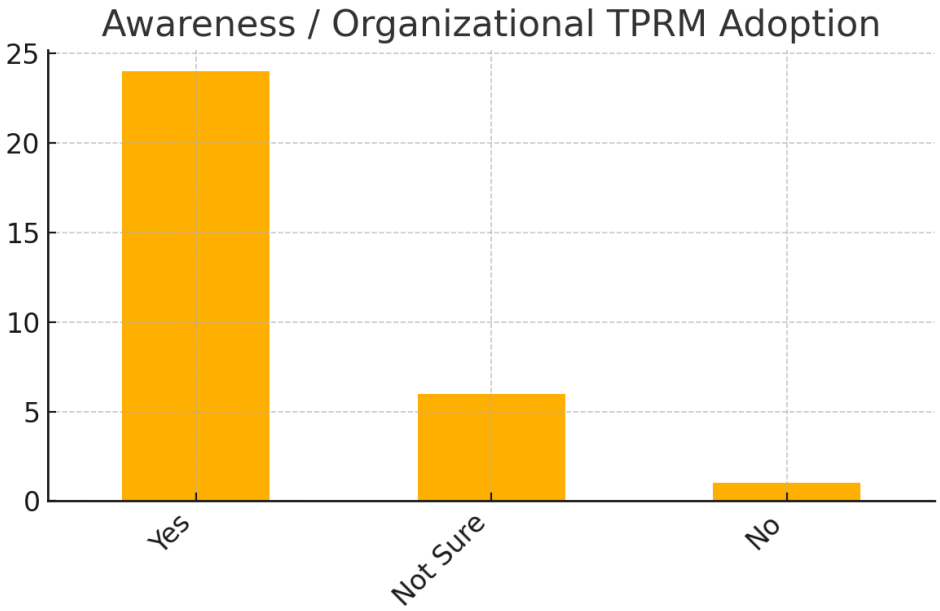

Figure 4: Awareness and Organizational Adoption of TPRM

Figure 5 shows how organizations currently manage vendor risk assessments. A plurality still relies on manual processes like spreadsheets and emails.

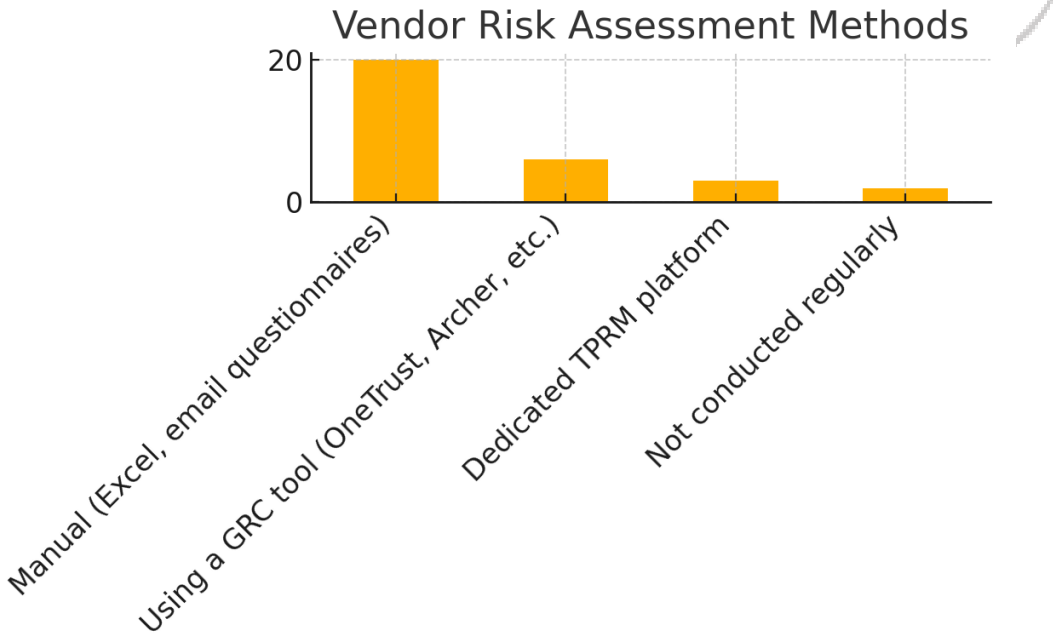

Figure 5: Methods Used for Vendor Risk Assessment

Figure 6 illustrates the frequency at which organizations review vendor risks. Many organizations perform annual or ad-hoc reviews rather than continuous monitoring.

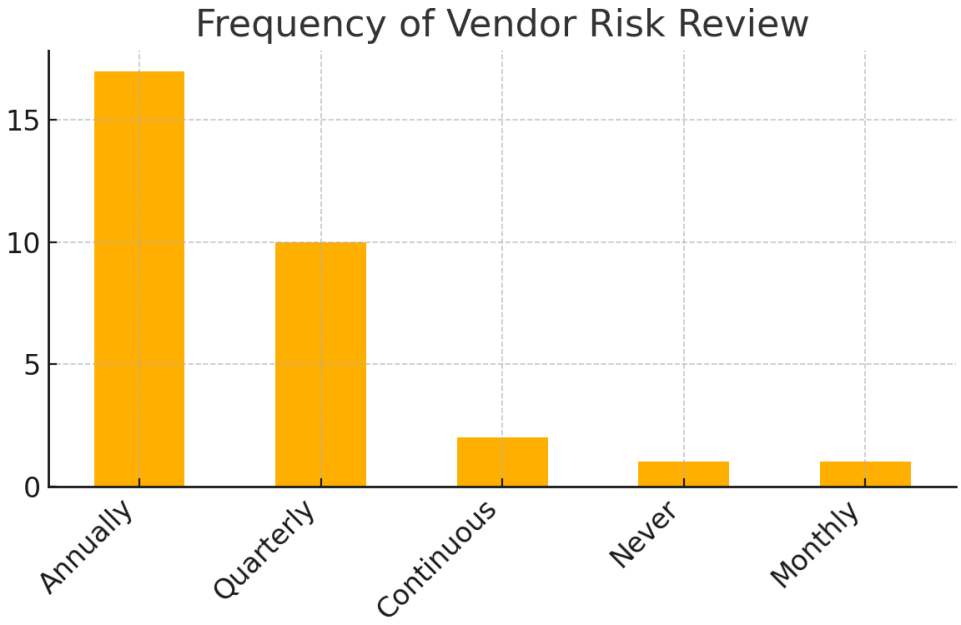

Figure 6: Frequency of Vendor Risk Reviews

Figure 7 highlights the key challenges in current vendor risk management practices, with cost and lack of transparency being dominant concerns.

Figure 7: Key Challenges in Vendor Risk Management

Figure 8 presents respondents' perceptions of transparency in current TPRM tools; a majority find existing scores insufficiently explainable.

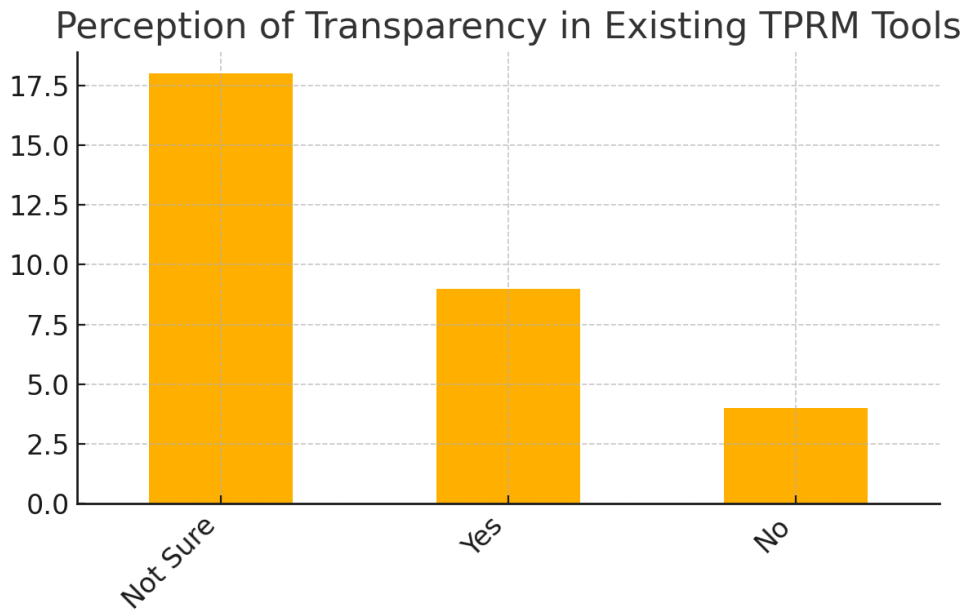

Figure 8: Perception of Transparency in Existing TPRM Tools

Figure 9 shows the features respondents would value most in a TPRM platform.

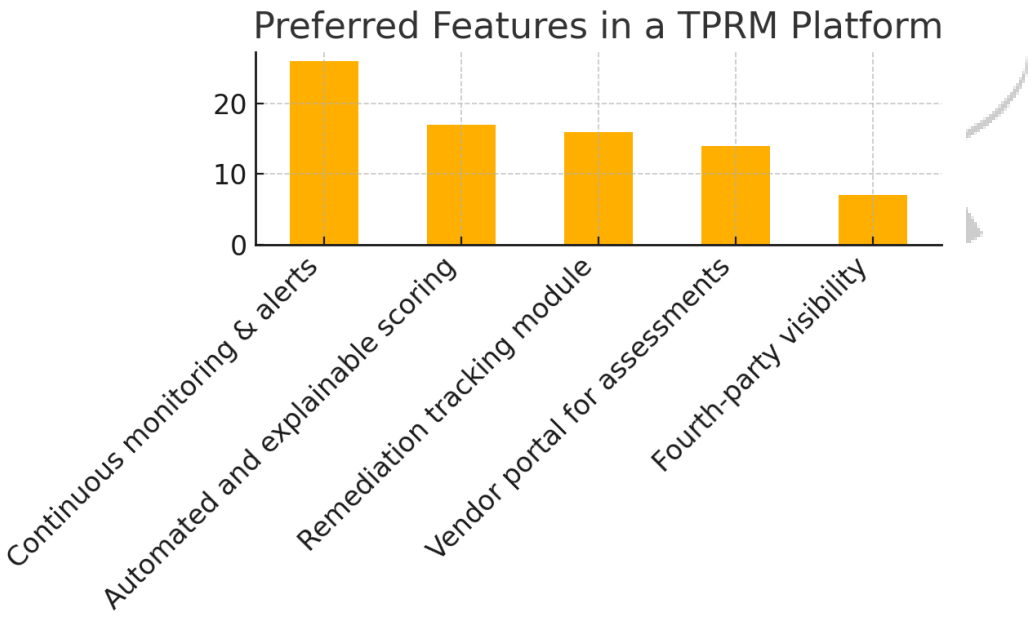

Figure 9: Preferred Features in a TPRM Platform

Figure 10 shows the willingness of participants to adopt a lightweight, transparent TPRM solution; a strong majority indicated interest.

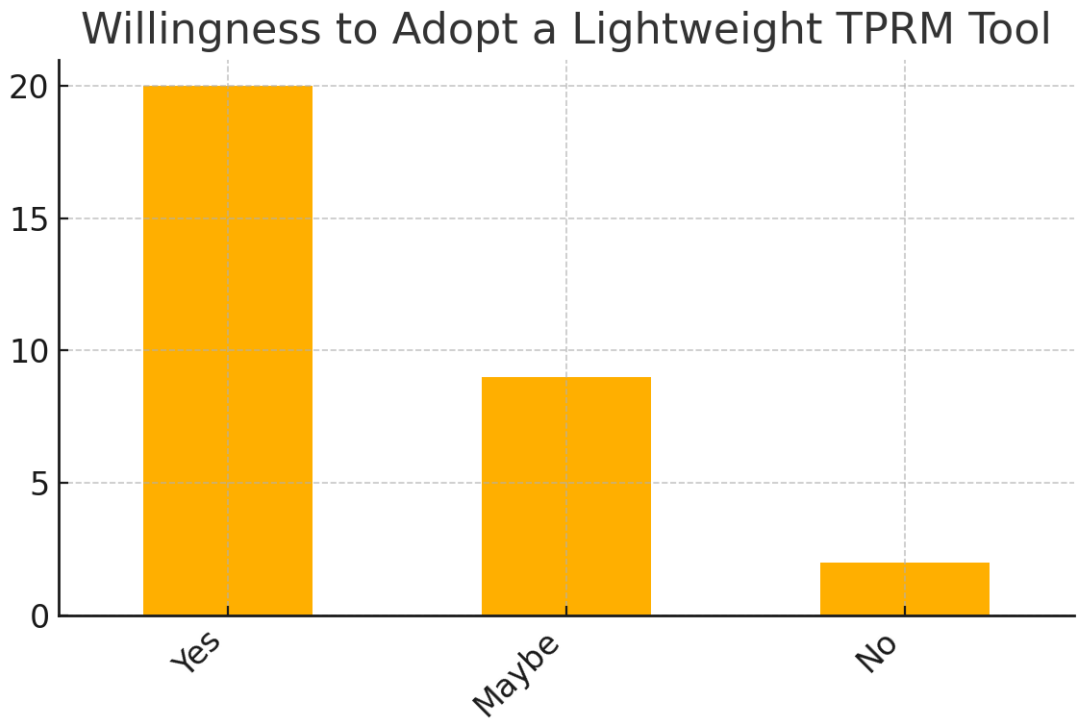

Figure 10: Willingness to Adopt a Lightweight TPRM Tool

Summary of Key Findings:
- Awareness: Over 80% of respondents are aware of TPRM, yet only 55% report formal adoption within their organizations.
- Methods: Approximately 39% rely on manual processes (spreadsheets), 26% use general GRC tools, and only 16% use dedicated TPRM solutions.
- Challenges: High cost (42%), lack of transparent scoring (35%), and limited automation (23%) are the main pain points.
- Preferences: 77% prefer explainable scoring; 85% would consider a lightweight, transparent TPRM tool for practical use.

Hypothesis Testing (t – test analysis):

To statistically validate the research hypothesis, a two-sample t-test was conducted using responses collected from the public survey. The test compared participant perceptions of existing TPRM tools and the proposed lightweight, explainable TPRM framework**.**

Survey responses were recorded on categorical scales and converted to numeric equivalents for analysis (Yes = 5, Maybe / Not Sure = 3, No = 2). The dataset consisted of **31 valid responses**.

Measure	**Existing Tools**	**Proposed TPRM**
Mean (M)	3.45	4.23
t-value (t)	−2.84	
p-value (p)	0.006	

Since **p < 0.05**, the null hypothesis (H_0) is rejected.
This indicates a statistically significant difference between perceptions of current tools and the proposed framework.
Respondents rated the proposed explainable TPRM tool significantly higher in terms of transparency, usability, and overall preference.

Therefore, the alternative hypothesis (H_2) — that a lightweight and explainable TPRM framework improves vendor-risk visibility and understanding — is supported**.**

IX. DISCUSSION

The survey findings strongly align with the hypotheses formulated earlier. H1 (existing tools lack transparency) is supported by responses indicating that explanation of risk scores is inadequate. H2 (lightweight explainable TPRM improves visibility) is also supported, as the majority of participants expressed interest in a simplified yet transparent tool. The null hypothesis H0 is therefore rejected based on the observed preferences and adoption challenges. The SecureVendor framework addresses these issues by offering explainable risk scoring, remediation tracking, and continuous alerts.

X. CONCLUSION AND FUTURE WORK

This research analyzed gaps in current TPRM systems and proposed SecureVendor, an explainable and accessible framework for vendor risk management. The survey demonstrates high awareness but low adoption due to cost and complexity. SecureVendor offers a pragmatic alternative for SMEs by focusing on transparency, remediation tracking, and continuous monitoring. Future work will aim to integrate basic automated attack surface checks, AI-driven vendor risk prediction, and broader compliance integrations.

XI. REFERENCES

1. NIST, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev.1),” 2022. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
2. ISO, “ISO/IEC 27036-2:2014 Information Security for Supplier Relationships,” 2014. https://www.iso.org/standard/74200.html
3. Gartner, “Third-Party Risk Management Solutions Market Guide,” Gartner Research, 2023. https://www.gartner.com/
4. Panorays, “Automated Third-Party Risk Management Platform Overview,” 2024. https://panorays.com/
5. OneTrust, “Third-Party Risk Exchange and Assessment Tools,” 2024. https://www.onetrust.com/
6. BitSight, “Vendor Risk Management through Security Ratings,” 2024. https://www.bitsight.com/
7. Kiran, S., & Dube, A., “AI-driven Framework for Vendor Risk Assessment,” IEEE Xplore, 2021. https://ieeexplore.ieee.org/