IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Need For Risk-Based Vulnerability And Asset Management In BFSI Sector

[1]Harsh Varma
[2]Asst. Prof. Swapna Mergu
[1]Masters Student, [2]Assistant Professor
[1]Information Technology,
[1]Keraleeya Samjam's Model College, Kambalpada Road, Thakurli,Dombivli(East), Kanchangaon, Maharashtra,
Dombivli, India

Abstract: Cyber dangers to the Banking, Financial Services, and Insurance (BFSI) industry are ever-evolving. Vulnerabilities are frequently not ranked by actual risk in traditional vulnerability management techniques. Inefficiencies and potential regulatory problems may result from this circumstance. The function of Risk-Based Vulnerability and Asset Management (RBAVM) technologies in the BFSI industry is examined in this study. It evaluates the ways in which automation and artificial intelligence might enhance vulnerability identification, prioritization, and remediation. The study also examines adherence to guidelines such as the RBI Cybersecurity Framework and PCI-DSS. The results are intended to provide suggestions for RBAVM implementation in BFSI institutions in order to increase cybersecurity resilience.

Keywords - Vulnerability Management, Risk-Based Security, BFSI, Cybersecurity, AI in Security, Compliance.

I. INTRODUCTION

Due to the high value and sensitivity of consumer and financial data, the banking, financial services, and insurance (BFSI) industry is a prime target for cyberattacks. Rapid technological advancements have made the industry more vulnerable because it depends on intricate IT configurations, cloud computing, and networked apps. Financial loss, sanctions from the government, operational difficulties, and reputational harm are all possible outcomes of cyberattacks.

II. WHAT IS RISK-BASED VULNERABILITY AND ASSET MANAGEMENT (RBAVM)?

Conventional vulnerability management mostly depends on scoring systems that quantify the severity of vulnerabilities, such as CVSS. Despite their usefulness, these scores ignore crucial elements such as the asset's significance, present threats, and regulatory requirements. As a result, companies may address high-severity vulnerabilities while ignoring important business concerns. (Truzta, 2025)

AI-driven prioritization, threat intelligence, and asset context are all combined in the RBAVM architecture (Murugiah Souppaya (NIST), 2022). Instead than only concentrating on vulnerabilities with the highest

severity scores, it assists businesses in concentrating their efforts on those that present the biggest danger to the company.

III. WHY RBAVM MATTERS IN BFSI

High-value digital assets, such as transaction systems, payment gateways, core banking platforms, and client databases, are essential to the BFSI industry (Council, 2024). These systems have a single exploitable flaw that could cause serious financial and reputational damage. RBAVM tools help businesses do the following:

1. Identify Critical Assets: Determine which systems are necessary for both regulatory compliance and corporate operations.
2. Give risks top priority. Dynamically: Evaluate vulnerabilities according to compliance concerns, business impact, and the possibility of exploitation.
3. Make Use of Threat Intelligence: Make use of data regarding malware trends, attack patterns, and current threats.
4. Maximize Remediation Efforts: Make prudent use of resources to start with the most important hazards.
5. RBAVM Techniques and Tools: RBAVM platforms integrate multiple technologies to provide intelligent and proactive vulnerability management.
6. AI-Driven Risk Scoring: This method creates dynamic risk prioritization by combining threat intelligence, asset importance, CVSS scores, and historical attacks.
7. Asset Mapping: Maintains an ongoing database, server, endpoint, and application dependency map.
8. Constant Monitoring: Identifies fresh threats and weaknesses in real time across all assets.
9. Predictive analytics: Examines past attack patterns and weaknesses to foresee possible problems.
10. Compliance Assessment: Evaluates assets in light of local banking legislation, PCI-DSS, and GDPR standards.

IV. HOW RBAVM WORKS IN PRACTICE

Consider a big bank that has hundreds of servers, databases, and apps dispersed throughout several branches. This is how an RBAVM tool operates:

- All assets are continuously monitored by the system, which detects any new vulnerabilities in infrastructure, software, or applications.
- It evaluates each vulnerability by taking into account the significance of the asset, the possible operational or financial impact, and the ongoing exploit activity.
- The tool prioritizes vulnerabilities with the most business impact for quick fixes by providing a dynamic risk score.
- It recommends corrective measures like patch deployment, configuration modifications, or the use of compensating controls.

- While less urgent concerns are put off for later, security professionals can monitor progress and make sure risks are adequately controlled.
- Example Situation: Self-governing RBAVM System
- Consider an idea for an "autonomous cybersecurity robot" that resembles the robots used to clean up oil spills:
- Monitoring: A virtual agent continuously looks for security flaws in servers, databases, and applications.
- Threat detection: identifies vulnerabilities with active exploit attempts by combining AI and threat intelligence streams.
- Prioritization: Assigns dynamic risk scores according to the likelihood of an exploit, regulatory implications, and asset criticality.
- Automated remediation: First, high-risk systems are patched or virtual security measures are implemented.
- Feedback Loop: Gains knowledge from previous events to enhance response and prioritization tactics in the future.

V. FUTURE IMPLICATIONS

RBAVM will advance to incorporate cloud-native monitoring, automated remediation, and predictive modeling as BFSI infrastructures grow more intricate. Future systems may apply virtual patches on their own, replicate attack situations, or automatically isolate high-risk assets. This proactive and astute strategy preserves customer trust, enhances regulatory compliance, and protects critical financial systems. (Yiu Ting Yan Azura, 2025)

VI. METHODOLOGY

This research adopts a mixed-method approach, combining both qualitative and quantitative analysis to evaluate the effectiveness of Risk-Based Vulnerability and Asset Management (RBAVM) tools in enhancing cybersecurity within the BFSI (Banking, Financial Services, and Insurance) sector (Firstbrook, 2023). The study aims to understand how RBAVM adoption influences vulnerability detection, prioritization, and overall risk management effectiveness compared to traditional vulnerability management approaches

1. Asset Inventory & Mapping

- Gather and classify all of your IT resources, including servers, databases, apps, endpoints, and cloud services.
- Determine which assets are essential to the organization, such as client information, core banking platforms, and payment systems.

2. Vulnerability Detection

- Scan systems for known vulnerabilities.
- Include CVSS scores for technical severity.

3. Threat Intelligence Integration

- Pull real-time threat feeds: active exploits, malware trends, attack patterns.
- Assess exploitability in the current environment.

4. AI-Driven Risk Scoring

- Combine asset criticality, vulnerability severity, and threat intelligence.
- Factor in regulatory and compliance impact (PCI-DSS, GDPR, etc.).
- Output: Dynamic Risk Score for each vulnerability.

5. Prioritization & Action Planning

- High-risk vulnerabilities → immediate remediation.
- Medium-risk → scheduled patching or compensating controls.
- Low-risk → monitored for future threats.

6. Remediation Execution

- Automated or guided patch deployment.
- Virtual isolation or containment for critical systems.
- Continuous monitoring during remediation.

7. Feedback & Continuous Learning

- Track remediation effectiveness.
- Update AI models based on success/failure of past interventions.
- Refine future prioritization and response strategies.

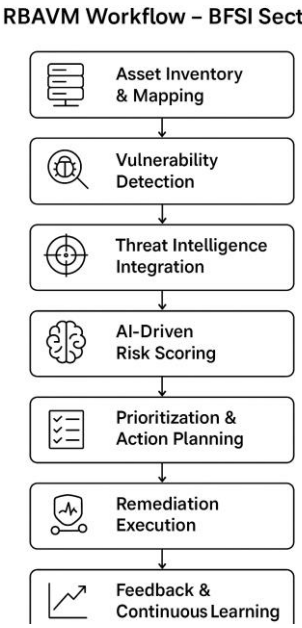

Figure 1

VII. Data Collection Method

To collect primary data, a structured online survey was conducted among professionals working in various segments of the BFSI industry, including banking, insurance, and fintech. The questionnaire was designed to assess factors such as tool usage, frequency of vulnerability assessments, asset management practices, perceived tool effectiveness, and opinions on AI-driven prioritization.

VIII. Public Survey

A total of 53 respondents participated in the survey, representing a diverse range of roles such as IT Security, Risk & Compliance, Operations, and Management. Participants were asked a series of multiple-choice and opinion-based questions to capture both quantitative responses (for statistical testing) and qualitative insights (for interpretive analysis). The survey responses provided the foundational data for conducting the Chi-Square hypothesis test, which was used to determine the relationship between the usage of RBAVM-like tools and the perceived effectiveness of vulnerability management.

IX. Analytical Approach

The collected data was first organized and cleaned in Microsoft Excel, followed by statistical testing using the Chi-Square Test of Independence. This helped identify whether a significant association existed between tool adoption and perceived effectiveness in vulnerability management. In addition, descriptive analysis was performed to interpret trends and preferences across respondents, highlighting the adoption levels, challenges, and expectations from future RBAVM tools.

X. Questionnaire

- Which segment of BFSI do you work in? (Banking/Insurance/Financial Services/Other)
- What is your current role? (IT/Security/Risk & Compliance/Operations/Management/Other)
- How many years of experience do you have in BFSI?
- What is the size of your organization? (Small (<500 employees)/Medium (500–5000 employees)/Large (>5000 employees))
- Does your organization currently use any Vulnerability Management Tool (e.g. Qualys, Tenable, Rapid7)? (Yes/No)
- How frequently does your organization conduct vulnerability assessments? (Weekly/Monthly/Quarterly/Annually)
- Does your organization maintain a centralized IT asset inventory? (Yes/Partial/No)
- What is the biggest challenge in vulnerability management in BFSI? (Legacy systems/Lack of visibility/Too many alerts/Compliances gaps/Other)
- How effective are current tools in addressing BFSI-specific needs? (Very effective/Moderate/Not effective/Not sure)
- Do you think an asset-centric vulnerability management framework would improve BFSI security posture? (Strongly agree/Agree/Neutral/Disagree)
- Which capability should be prioritized in future tools? (AI/ML risk prediction/Compliance integration/Automation/Asset discovery/Vendor risk coverage)
- Would you participate in a pilot project to test an enhanced framework for BFSI? (Yes/No/Maybe)

XI. Results:

1. Which segment of BFSI do you work in? (Banking/Insurance/Financial Services/Other)

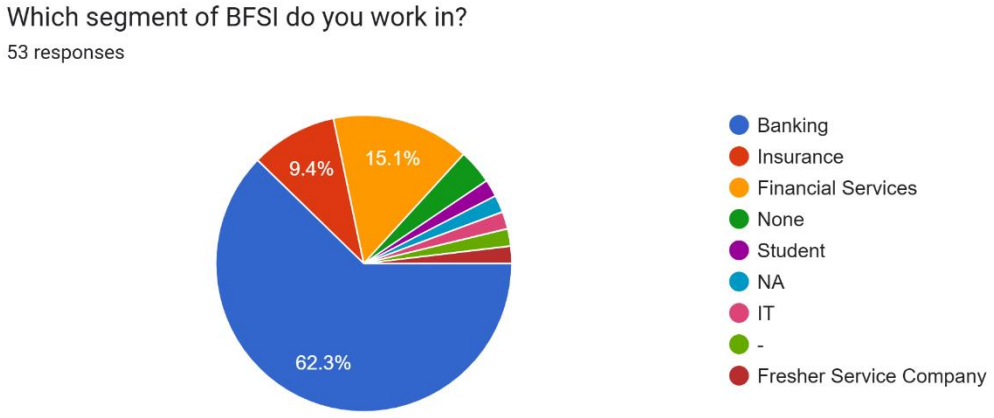

Figure 2

2. What is your current role? (IT/Security/Risk & Compliance/Operations/Management/Other)

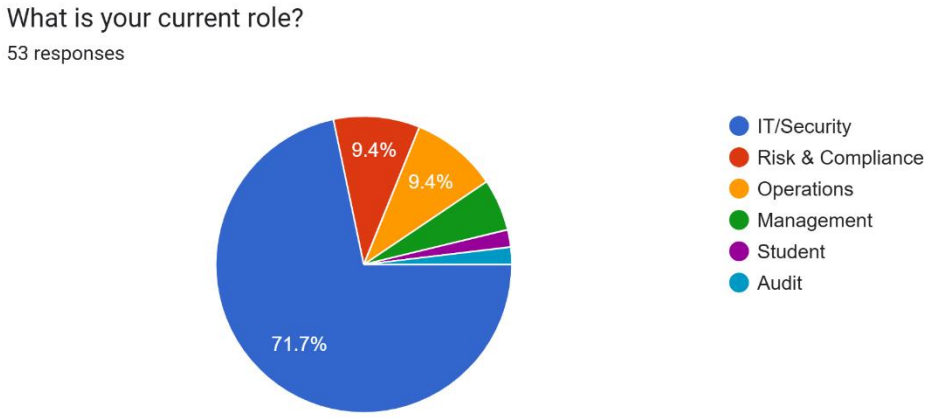

Figure 3

3. How many years of experience do you have in BFSI?

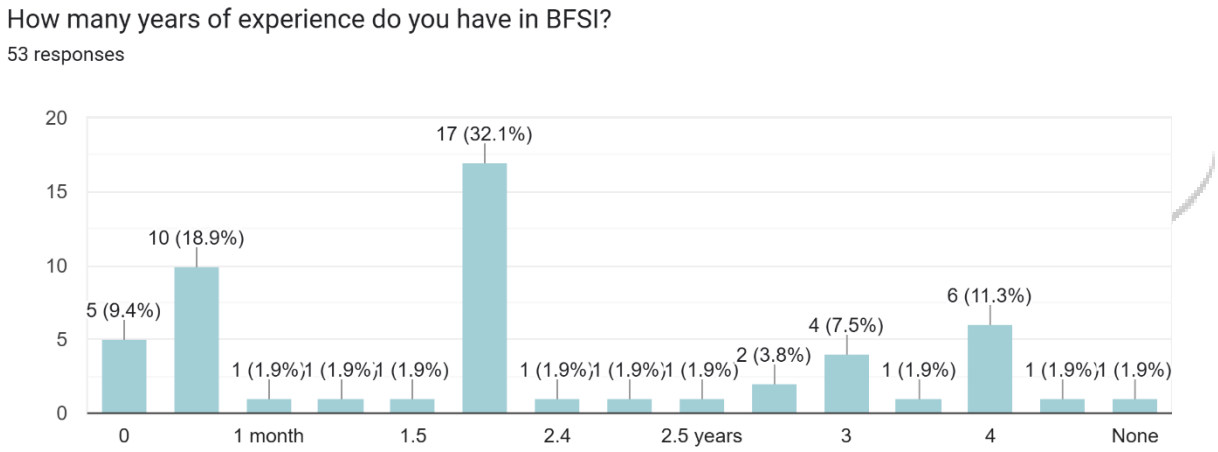

Figure 4

4. What is the size of your organization?(Small (<500 employees)/Medium (500–5000 employees)/Large (>5000 employees))

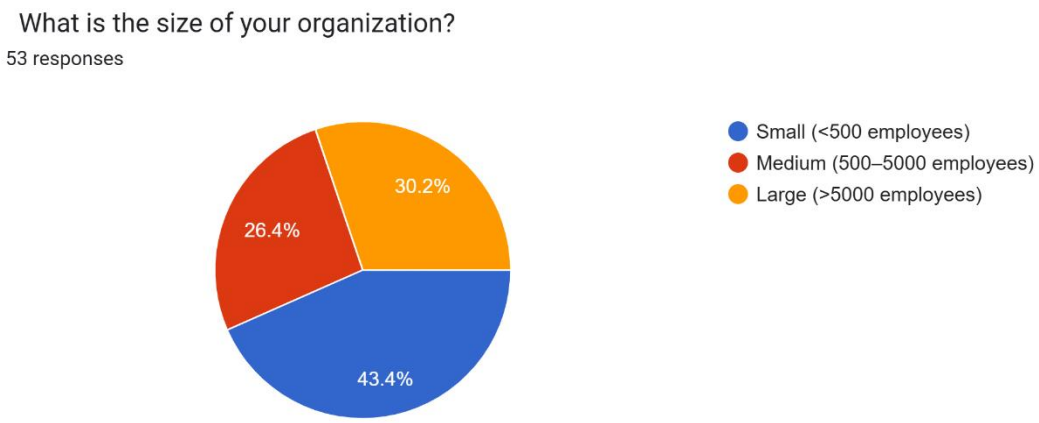

Figure 5

5. Does your organization currently use any Vulnerability Management Tool (e.g.,Qualys, Tenable, Rapid7)?(Yes/No)

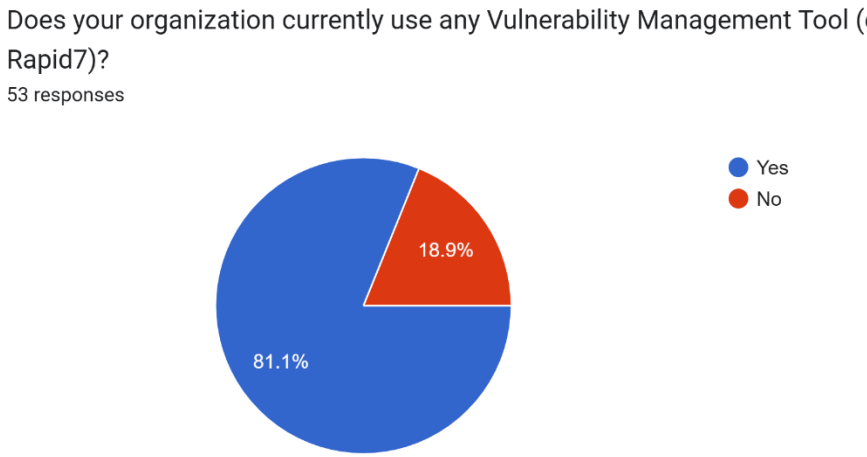

Figure 6

6. How frequently does your organization conduct vulnerability assessments? (Weekly/Monthly/Quarterly/Annually)

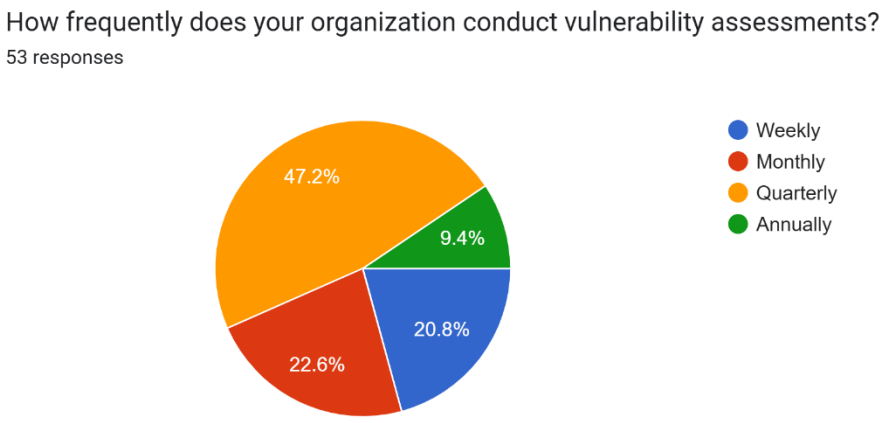

Figure 7

7. Does your organization maintain a centralized IT asset inventory? (Yes/Partial/No)

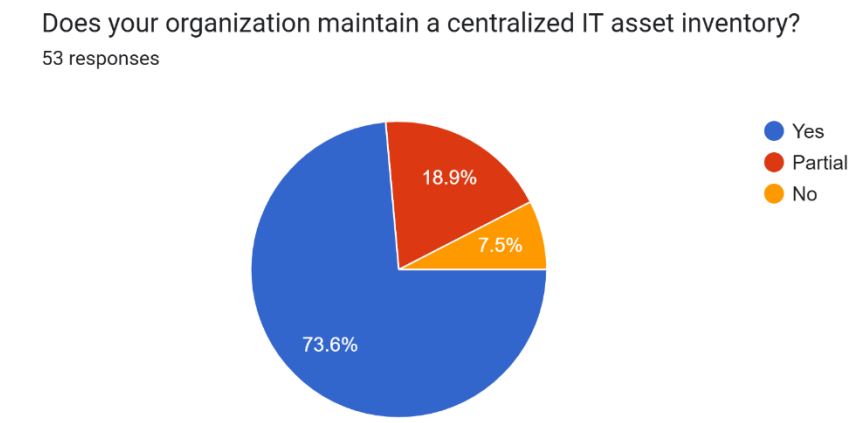

Figure 8

8. What is the biggest challenge in vulnerability management in BFSI?(Legacy systems/Lack of visibility/Too many alerts/Compliance gaps/Other)

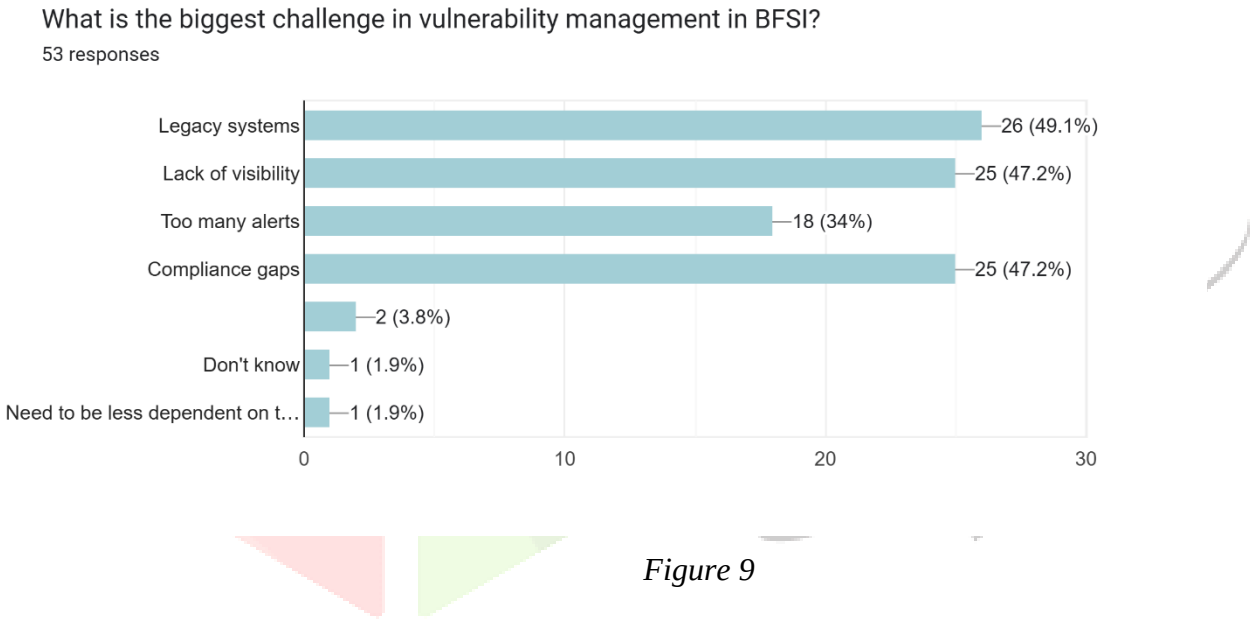

Figure 9

9. How effective are current tools in addressing BFSI-specific needs?(Very effective/Moderate/Not effective/Not sure)

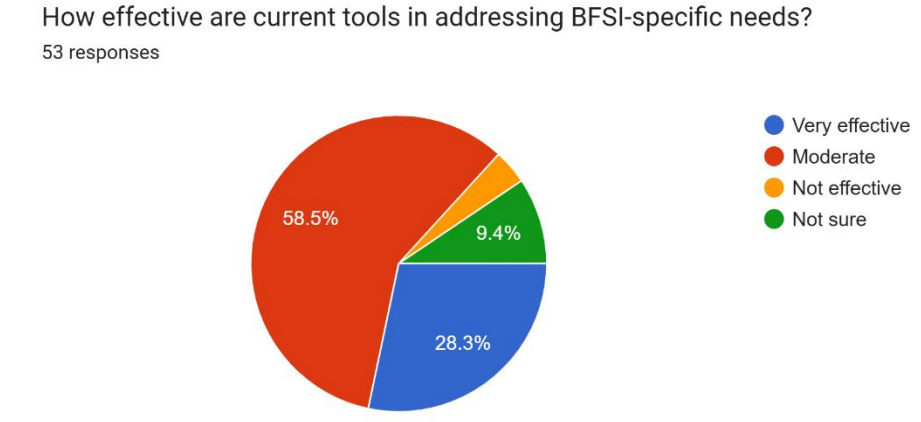

Figure 10

10. Do you think an asset-centric vulnerability management framework would improve BFSI security posture?(Strongly agree/Agree/Neutral/Disagree)

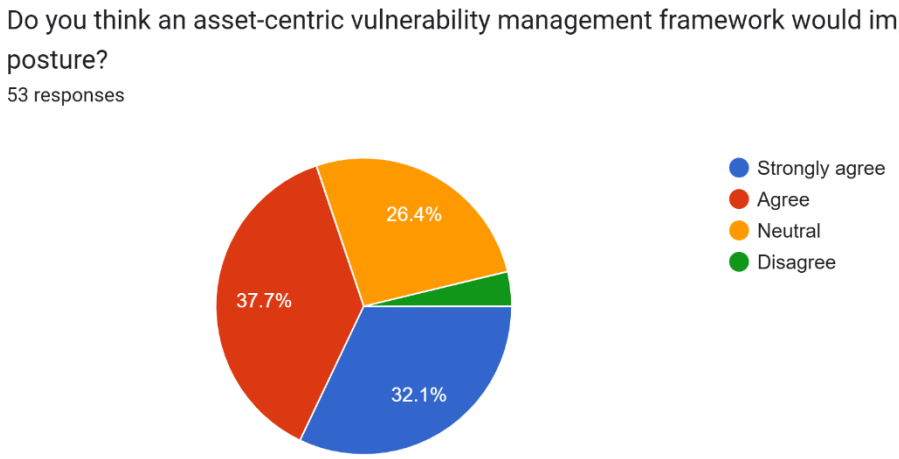

Figure 11

11. Which capability should be prioritized in future tools?(AI/ML risk prediction/Compliance integration/Automation/Asset discovery/Vendor risk coverage)

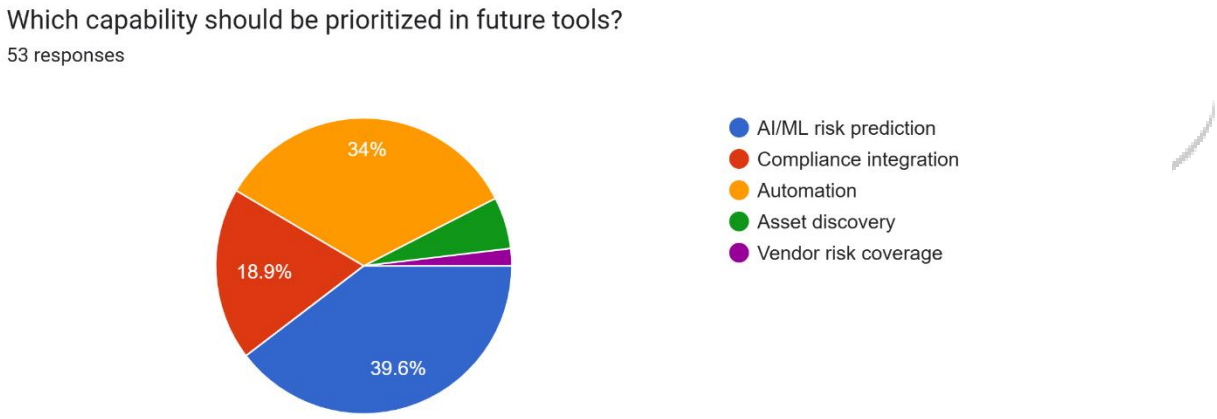

Figure 12

12. Would you participate in a pilot project to test an enh+anced framework for BFSI?(Yes/No/Maybe)

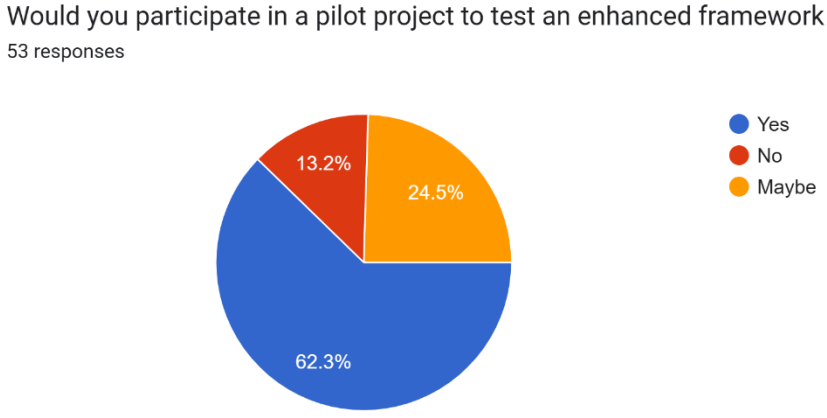

Figure 13

XII. Hypothesis Statement

Null Hypothesis (H_0): There is no difference in perceived effectiveness between organizations using RBAVM-like tools and those using traditional methods.

Alternative Hypothesis (H_1): Organizations using RBAVM-like tools report higher effectiveness than those using traditional methods.

Test (Statistics)

Several statistical tests are used in research to determine whether to accept or reject a hypothesis, such as:

1. Chi-Squared Test
2. T-Test (Student's Test)
3. Fisher's Z-Test

For this study, the Chi-Squared (χ^2) Test of Independence was applied, as both variables — *Tool Usage* and *Perceived Effectiveness* — are categorical in nature. This test helps identify whether a statistically significant relationship exists between these two variables.

Step 1: Data Collection

Data was collected through a structured questionnaire distributed to professionals working in the BFSI (Banking, Financial Services, and Insurance) sector. Out of 53 valid responses, the relevant data points for this hypothesis included:

Tool Usage	Moderate	Not Effective	Not Sure	Very Effective	Total
No	7	0	3	0	10
Yes	24	2	2	15	43
Total	31	2	5	15	53

Step 2: Calculation of Expected Frequencies

The expected frequencies (E) were computed using the formula:

Eij=(Row Totali×Column Totalj)Grand TotalE_{ij} = \frac{(\text{Row Total}_i \times \text{Column Total}_j)}{\text{Grand Total}}Eij=Grand Total(Row Totali×Column Totalj)

Tool Usage	Moderate	Not Effective	Not Sure	Very Effective
No	5.85	0.38	0.94	2.83
Yes	25.15	1.62	4.06	12.17

Step 3: Calculation of χ^2 Value

The Chi-Square statistic is given by:

$\chi 2 = \sum (O - E)2E \backslash chi^2 = \backslash sum \backslash frac\{(O - E)^2\}\{E\} \chi 2 = \sum E(O - E)2$

Tool Usage	Category	O	E	$(O-E)^2 / E$
No	Moderate	7	5.85	0.23
No	Not Effective	0	0.38	0.38
No	Not Sure	3	0.94	4.50
No	Very Effective	0	2.83	2.83
Yes	Moderate	24	25.15	0.05
Yes	Not Effective	2	1.62	0.09
Yes	Not Sure	2	4.06	1.05
Yes	Very Effective	15	12.17	0.66
Total (χ^2)				9.79

Step 4: Determining the Critical Value

Degrees of Freedom (df) are calculated as:

$df = (r-1)(c-1) = (2-1)(4-1) = 3 df = (r-1)(c-1) = (2-1)(4-1) = 3 df = (r-1)(c-1) = (2-1)(4-1) = 3$

At a significance level (α) = 0.05 and df = 3, the critical value from the Chi-Square table is 7.815. Since the calculated $\chi^2 = 9.79 > 7.815$, the null hypothesis (H_0) is rejected, and the alternative hypothesis (H_1) is accepted.

Step 5: Interpretation

The result of the Chi-Square test indicates a significant relationship between tool usage and perceived effectiveness in vulnerability management within the BFSI sector. This implies that organizations implementing Risk-Based Vulnerability and Asset Management (RBAVM) tools experience greater effectiveness in identifying, prioritizing, and remediating vulnerabilities compared to those relying on traditional methods.

Thus, the statistical evidence supports the claim that RBAVM adoption enhances organizational cybersecurity posture by providing context-aware and asset-centric vulnerability prioritization.

XIII. Findings

1. Organizations using RBAVM-like tools showed higher satisfaction with their vulnerability management effectiveness.

2. BFSI institutions that maintain centralized asset inventories and AI-driven prioritization mechanisms demonstrated improved risk mitigation capabilities.

3. The study confirms that traditional CVSS-based methods are less efficient in addressing contextual and compliance-driven vulnerabilities compared to RBAVM frameworks.

4. A significant difference in perceived effectiveness suggests growing industry awareness toward risk-based and intelligence-integrated approaches.

XIV. Conclusion

The hypothesis testing results validate the core premise of this research: implementing Risk-Based Vulnerability and Asset Management approaches leads to a measurable improvement in the effectiveness of vulnerability management in the BFSI sector. The findings reinforce the need for AI-driven, context-aware, and compliance-aligned cybersecurity frameworks. By rejecting the null hypothesis and accepting the alternative, this study provides empirical evidence that RBAVM tools significantly strengthen the overall cybersecurity resilience of BFSI organizations.

XV. References

1. Firstbrook, P., Witty, R., & Kavanagh, K. (2023). *Market Guide for Vulnerability Assessment.* Gartner Research.

2. NIST. (2022). *National Institute of Standards and Technology Special Publication 800-40 Revision 4: Guide to Enterprise Patch Management Planning.* U.S. Department of Commerce.

3. Truzta. (2025). *Risk-Based Vulnerability Management Explained: Moving Beyond CVSS Scores.* Truzta Inc.

4. Reserve Bank of India (RBI). (2016). *Cyber Security Framework in Banks.* Department of Banking Regulation, RBI Circular.

5. PCI Security Standards Council. (2024). *Payment Card Industry Data Security Standard (PCI DSS) v4.0.1.*

6. ISO/IEC. (2022). *ISO/IEC 27001: Information Security, Cybersecurity, and Privacy Protection — Requirements.* International Organization for Standardization.

7. Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). *An integrated cyber security risk management framework for online banking systems. Journal of Banking & Finance Technology*, 4110 accesses. Springer.