**From Framework to Practice: Barriers and Enablers to RMF Adoption in Mid-Sized Enterprises**

**Abstract**

*This study investigates the barriers and enablers influencing the adoption of the Risk Management Framework (RMF) in mid-sized software development enterprises through a quantitative research design. Four datasets were analyzed:  the Stack Overflow Developer Survey, ENISA Threat Landscape Reports, OpenSSF Secure Practices Survey, and Verizon’s Data Breach Investigations Report (DBIR). The study employed descriptive statistics to explore awareness patterns, exploratory factor analysis to identify latent barriers, binary logistic regression to model enablers, and independent t-tests to evaluate security performance outcomes. Findings reveal that RMF awareness is highest among DevOps Engineers and Software Architects (73.3%), yet practical adoption remains limited, with only 34.4% of Asian firms implementing RMF-aligned practices. Lack of leadership support emerged as the strongest barrier (loading = -0.58), while leadership endorsement was the most significant enabler (β = 1.1671, p < .001). Organizations that adopted RMF demonstrated 40% faster threat detection and 66% faster incident response compared to non-adopters. The study highlights the strategic role of leadership commitment, workforce training, and CI/CD pipeline integration in promoting RMF adoption. It recommends contextual RMF toolkits tailored for Agile environments, executive-level cybersecurity briefings, and role-specific certifications to accelerate adoption. By strengthening operational resilience and regulatory compliance, RMF offers a scalable pathway for mid-sized firms navigating the complexities of modern software security risks.*

**Keywords:** **Risk Management Framework (RMF), mid-sized enterprises, software security, quantitative analysis, risk governance adoption**

**1. Introduction**

In the contemporary digital economy, software development enterprises are increasingly vulnerable to cyber threats, regulatory demands, and complex operational risks. Mid-sized enterprises, in particular, occupy a precarious position: lacking the extensive resources of large corporations yet confronting comparable security threats. This context necessitates the adoption of a structured, anticipatory risk governance model. According to Ross (2018), the Risk Management Framework (RMF), developed by the National Institute of Standards and Technology (NIST), offers a standardized methodology for identifying, assessing, and mitigating risks throughout the software development life cycle (SDLC). While RMF has gained recognition for its integration of security, privacy, and cyber supply chain considerations into system development, its adoption among mid-sized software firms remains disproportionately low (Ross, 2018).

Jiang et al. (2024) avers that the principal constraint lies in the discrepancy between RMF's conceptual rigor and its practical viability in smaller-scale IT environments. For instance, a 2023 report by CloudBees indicates that although 83% of organizations are implementing structured software engineering practices, including platform engineering, many face significant challenges in full realization of these practices (CloudBees, 2023). RMF, alongside the Secure Software Development Framework (SSDF), is frequently perceived as abstract and resource-intensive, reducing its operational appeal for mid-sized enterprises.

Further compounding these limitations are technological and financial constraints. Turgay and Aydin (2023) notes that mid-sized firms often lack the technical expertise and infrastructure required to integrate RMF into their extant SDLC processes. These technical limitations are aggravated by the lack of tailored guides and contextual toolkits capable of adapting RMF to distinct legacy systems or customized configurations. Financial barriers are equally pronounced, Oko-Odion and Omogbeme (2025) argues that the initial financial outlay for RMF, encompassing workforce training, technological upgrades, and staff development, can be prohibitive, particularly for firms with constrained cybersecurity budgets.

Despite increased global cybersecurity spending, which reached USD 90 billion in 2024 among small and mid-sized businesses according to Agrawal (2022), there remains a proclivity toward fragmented, piecemeal security investments over comprehensive, governance-centric frameworks. This phenomenon results from the compounded effects of limited internal capabilities, workforce shortages, and the perceived complexity of aligning RMF with existing operational workflows.

Concurrently, notable cyber incidents have accentuated the urgency for systemic risk management. High-profile cases such as the SolarWinds attack in 2020 and the exploitation of the Log4j vulnerability in 2021 illustrate how vulnerabilities in ubiquitous software components can trigger widespread disruption across interconnected systems (STAHIE, 2022). These incidents have disproportionately affected mid-sized enterprises, many of which depend on third-party software vendors without implementing rigorous risk assessments or due diligence procedures. This underscores the imperative of continuous monitoring, third-party evaluation, and secure coding—core tenets of RMF that are critical yet often difficult to operationalize in resource-constrained environments.

Organizational dynamics act as substantial impediments to RMF adoption; Park et al. (2004) revealed that even security-conscious mid-sized firms frequently fail to institutionalize risk management due to vague implementation strategies and inadequate internal capacity. Management engagement is frequently inconsistent, and roles associated with risk governance are ambiguously defined. Bhatia and Gabhane (2025) similarly documents the experience of a mid-sized firm hindered by fluctuating technical requirements and the absence of formalized risk controls. These challenges are amplified in agile environments, where frequent iterations reduce the perceived utility of rigid risk protocols. Moreover, Ojiako et al. (2024) found that geographical dispersion and communication breakdowns in distributed teams exacerbate the difficulty of embedding RMF practices.

Although Ross (2018) advocates for embedding risk governance into the foundational stages of system design, the practice remains largely aspirational among mid-sized firms. Security is often relegated to the post-development stage, undermining the intended security-by-design philosophy and thereby diminishing the effectiveness of RMF implementation.

Nonetheless, the strategic adoption of RMF holds substantial promise for mid-sized software development enterprises. When effectively implemented, RMF can strengthen software security postures, enhance regulatory compliance, and improve client trust, all of which contribute to mitigating reputational and financial risks associated with breaches (Arundhati, 2025). Factors enabling successful adoption include dedicated leadership, accessible and contextualized RMF guidance materials, and sustained investment in workforce training oriented around risk-centric development (Insight Assurance, 2024). Notably, the shift toward platform engineering provides a potential integration vector. The CloudBees (2023) report indicates that 20% of surveyed firms have fully adopted platform engineering, reflecting an emerging standardization that could facilitate RMF assimilation.

The following chart provides a comparative visualization of cybersecurity performance metrics before and after the adoption of the Risk Management Framework (RMF) in mid-sized software development enterprises. Synthesized from empirical study such as the Log4j and SolarWinds incidents, the data highlights measurable improvements in key areas such as incident response time, vulnerability remediation rate, and compliance audit scores. These enhancements reflect the practical benefits of embedding RMF principles into secure software development processes.



***Figure 1: Impart of RMF on Cybersecurity Performance***

Projections for the global integrated risk management software market support these developments. Straits Research (2023) estimated its value at USD 10.9 billion, forecasting a rise to USD 12.5 billion by 2032, at a 15.1% compound annual growth rate. Yet despite favorable market trends, many small and mid-sized enterprises persist with reactive, improvised strategies. Empirical evidence by Liang et al. (2023) shows that integrating continuous risk assessments within DevOps workflows significantly enhances threat detection and reduces remediation timelines. These findings affirm that RMF-aligned practices, when adapted to organizational constraints, offer both strategic and operational advantages. This study addresses a critical gap by examining barriers and enablers to RMF adoption in mid-sized software enterprises through rigorous statistical methods, including exploratory factor analysis, logistic regression, and t-tests. It contributes practical insights by proposing contextualized RMF adoption strategies for Agile environments. Additionally, the study references ISO/IEC 27005 to strengthen its theoretical foundation and standardizes statistical reporting for clarity, ensuring relevance for both academic and industry audiences. This research aims to investigate the barriers and enablers influencing the adoption of Risk Management Framework (RMF) in mid-sized enterprises within the software development context, and to provide insights for improving RMF implementation strategies for this specific organizational group, by achieving the following objectives:

1. Examines the level of awareness and current adoption practices of RMF among mid-sized software development enterprises.
2. Identifies the organizational, technical, and financial barriers that hinder the effective implementation of RMF in software engineering processes.
3. Explores the enabling factors—such as leadership support, staff capability, and integration with SDLC tools—that facilitate RMF adoption in software development.
4. Evaluates the extent to which RMF adoption contributes to improved software security posture and risk mitigation outcomes in mid-sized enterprises.

## **2. Literature Review**

In the context of software development, risk is conventionally defined as the probability of an event or condition adversely affecting project or organizational objectives (Kitsios et al., 2022). Leading standards offer distinct, yet complementary, interpretations. The National Institute of Standards and Technology (NIST) defines risk as “a measure of the extent to which an entity is threatened by a potential circumstance or event,” with emphasis placed on both likelihood and potential impact (Ross, 2018; Ajayi et al., 2025). In contrast, ISO 31000 conceptualizes risk as “the effect of uncertainty on objectives,” thereby broadening its scope beyond technical threats to encompass strategic and operational concerns (Tranchard, 2018; Balogun, 2025). According to Khan et al. (2022), within software engineering, risk encompasses not only information security vulnerabilities but also inefficiencies in development processes and disruptions to operational continuity.

A meaningful distinction exists between project risk and security risk, though their boundaries often intersect. Project risk pertains to uncertainties associated with development timelines, budget allocations, or deliverable quality and is typically managed through conventional project management techniques (Taherdoost, 2024; Kolade et al., 2025). Security risk, on the other hand, focuses on safeguarding information systems, involving threats arising from software defects, architectural weaknesses, or hostile intrusion attempts (Shokunbi et al., 2024; Metibemu et al., 2025). Risk categories converge during the Software Development Life Cycle (SDLC), thus requiring integrated risk management approaches that bridge both project governance and cybersecurity (Saeed et al., 2024; Obioha-Val, 2025).

The evolving conceptualization of software risk has shifted toward a multidimensional understanding. George et al. (2024) argues that modern risk vectors now encompass technical malfunctions, dependency on third-party services, operational downtimes, and reputational harm resulting from public exposure to security incidents. A technical defect may serve as the initial risk point, yet its exploitation can escalate into substantial business disruption and reputational damage. Botti-Lodovico et al. (2021) emphasized early detection and preemptive action as foundational to secure and high-quality software systems, an assertion reaffirmed by contemporary frameworks (Khan et al., 2022; Olutimehin, 2025).

According to Ross (2018), NIST’s Risk Management Framework (RMF) offers a methodical model for embedding security throughout the SDLC, structured into seven phases: prepare, categorize, select, implement, assess, authorize, and monitor. This is supplemented by the Secure Software Development Framework (SSDF), which provides practical measures such as threat modeling, secure coding, and vulnerability control to reinforce RMF’s strategic mandate (Souppaya et al., 2022; Oyekunle et al., 2025). Rather than serving as a substitute, SSDF augments RMF through tactical implementation (NIST, 2021; Salako et al., 2025).

Nonetheless, mid-sized software enterprises often struggle with RMF implementation. Bhardwaj (2024) asserts that unlike larger corporations equipped with compliance infrastructures or micro-startups willing to accept higher risk for agility, mid-sized firms operate under resource constraints and iterative workflows (Alam et al., 2024; Alao et al., 2024). Despite increased adoption of cloud platforms and DevOps methodologies, comprehensive risk governance remains limited, primarily due to cost pressures and difficulties with framework integration (OECD, 2024; Tiwo et al., 2025). Effective RMF deployment in these contexts necessitates flexible, scalable implementations tailored to organizational realities.

**RMF Adoption: Awareness and Current Practices**

Awareness of the Risk Management Framework (RMF) has expanded significantly across the software development sector, reflecting the growing emphasis on secure engineering practices and compliance with regulatory standards. According to CloudBees (2023) approximately 83% of organizations are engaging with structured development methodologies, including frameworks aligned with RMF principles. Nevertheless, only 20% have succeeded in fully operationalizing such practices, revealing a notable disparity between conceptual awareness and practical application. SHRM (2022) avers that this implementation gap is particularly pronounced within mid-sized enterprises, where formalized training in risk governance remains limited and underfunded.

Although NIST publications, most notably SP 800-37 Rev. 2, have sought to demystify RMF processes, the framework is still largely perceived by mid-tier firms as applicable only to highly regulated government or defense sectors (Ross, 2018). This perception, combined with the technical density of RMF documentation, hinders broader comprehension and adoption across less formal organizational environments (Fabius & Graubart, 2014; Balogun et al., 2025).

Moreover, Al-Baik et al. (2024) observes that software development education often neglects comprehensive instruction in structured risk management, thereby compounding these challenges at the workforce level. In practice, many mid-sized organizations apply RMF in fragmented ways. Rather than executing the full sequence—prepare, categorize, select, implement, assess, authorize, and monitor—firms may implement isolated components such as vulnerability scanning or threat modeling. Block (2023) reported on such partial adoption, noting the integration of risk controls into agile sprints without accompanying governance mechanisms. Malamas et al. (2021) similarly documented the absence of formal authorization and continuous monitoring despite ongoing risk assessment efforts. Conversely, Liang et al. (2023) demonstrated that continuous risk assessment embedded into DevOps pipelines yielded superior threat responsiveness and shorter remediation times.

Sector-specific imperatives also shape RMF adoption. Oyewole et al. (2024) posits that fintech firms, due to heightened regulatory exposure and data sensitivity, tend to adopt comprehensive risk frameworks, whereas mid-sized health tech firms may instead prioritize compliance with standards such as HIPAA. Organizational maturity, client expectations, and budgetary constraints influence RMF implementation practices (Stoltz, 2024; Obioha-Val et al., 2025). Agrawal (2022) and OECD (2023) confirm that although technological adoption is accelerating, structured risk governance remains inconsistent among mid-sized enterprises due to integration complexity and limited financial resources. These findings underscore the necessity of adapting RMF methodologies to the specific operational realities of mid-sized software development environments.

**Barriers to RMF Adoption in Software Engineering**

The implementation of the Risk Management Framework (RMF) within mid-sized software engineering enterprises is consistently constrained by a convergence of organizational, technical, and financial barriers. Aladayleh and Aladaileh (2024) contends that a primary organizational impediment is the lack of executive commitment, which significantly diminishes the prioritization of structured risk governance efforts. As observed by Bhatia and Gabhane (2025), insufficient leadership endorsement relegates RMF initiatives to peripheral concerns, impeding comprehensive integration into development operations. This issue is compounded by fragmented interdepartmental communication, procedural inertia, and siloed organizational structures that obstruct the cross-functional collaboration essential for holistic risk management.

Structural deficiencies also arise from the absence of dedicated security governance units. Staffler (2021) observes that, unlike larger enterprises equipped with formal compliance departments, many mid-sized firms assign cybersecurity responsibilities ambiguously across multifunctional teams. This lack of clear accountability undermines the consistency of RMF implementation, particularly in its latter stages—assessment, authorization, and monitoring. The misalignment between organizational culture and formal risk protocols leads to erratic enforcement and diminished operational coherence (Akinsola, 2025; Olutimehin, 2025).

From a technical standpoint, integrating RMF into Agile and DevOps methodologies presents a substantial challenge. These paradigms prioritize speed, flexibility, and continuous delivery, in direct contrast to the RMF’s sequential, documentation-intensive structure (Masud et al., 2022; Salami et al., 2025). NIST (2023) argues that this procedural incompatibility limits RMF’s applicability within dynamic development environments. Additional complications stem from legacy systems and outdated technical architectures that require significant adaptation to conform to RMF-prescribed control standards. The limited availability of automation tools for risk assessment and control implementation further exacerbates the difficulty, rendering manual execution both time-consuming and error-prone (Pandey et al., 2022; Tiwo et al., 2025).

Financial constraints represent another critical barrier; the upfront investment required for RMF adoption, comprising staff training, tool acquisition, and third-party audits, can be prohibitive for mid-sized firms (Tavasoli et al., 2025; Balogun et al., 2025). Despite reported growth in global SME cybersecurity spending to USD 90 billion these investments tend to favor tactical, fragmented solutions rather than comprehensive governance frameworks (Agrawal, 2022; Obioha-Val et al., 2025). Crovini et al. (2020) further note that although SMEs demonstrate awareness of risk management, financial limitations hinder the institutionalization of formal structures. These findings underscore the necessity for context-sensitive adaptations of RMF that align with the fiscal and operational capacities of mid-market software enterprises.

**Enablers of RMF Adoption in Software Development**

The successful adoption of the Risk Management Framework (RMF) within mid-sized software development enterprises is contingent upon a confluence of organizational commitment, skilled personnel, and the seamless integration of technology. Yuguda et al. (2023) argues that one of the most significant enablers is strategic leadership support, which positions RMF not merely as a regulatory obligation but as a strategic imperative embedded within the enterprise’s risk and operational framework. According to Jerab and Mabrouk (2023), executive endorsement plays a critical role in aligning RMF objectives with broader organizational goals by ensuring the allocation of resources and the creation of formal accountability mechanisms. FasterCapital (2025) further emphasizes the value of “risk champions”—designated individuals or units that advocate for RMF and mediate between leadership and technical implementation teams. Their role is pivotal in cultivating a governance-oriented culture that supports consistent risk practices across the software development life cycle.

Equally foundational is the capacity of the workforce; developers proficient in secure coding techniques, threat modeling, and vulnerability mitigation are indispensable to embedding RMF throughout the software development lifecycle (Czekster, 2024; Olutimehin, 2025). Liang et al. (2023) notes that firms which invest in developer education oriented around risk-centric competencies are more effective in integrating RMF within Agile and DevOps environments. However, technical acumen alone is insufficient. Cross-functional collaboration between software engineers, DevOps specialists, and security professionals is essential for ensuring that risk evaluation and control implementation occur iteratively—from design to deployment (Liang et al., 2023; Czekster, 2024; Balogun et al., 2025). Such collaboration mitigates the fragmented application of RMF and enables its contextual adaptation.

Technological integration further enhances RMF operationalization; embedding RMF elements within existing tools—such as Git for version control, JIRA for project tracking, and Jenkins for continuous integration—enables partial automation of control mapping, documentation, and compliance verification (Github, 2024; Balogun et al., 2025). Platform engineering, with its emphasis on governance and automation, supports RMF-aligned workflows (Agrawal, 2022; Olutimehin et al., 2025). Continuous monitoring capabilities within CI/CD pipelines reinforce compliance through real-time risk visibility and metrics tracking, transforming risk governance from an episodic to a continuous practice. When these organizational, human, and technological factors converge, RMF implementation becomes both scalable and sustainable in mid-sized software development enterprises.

**Outcomes and Benefits of RMF Adoption**

The adoption of the Risk Management Framework (RMF) in software development environments yields significant outcomes that extend well beyond compliance obligations, contributing to enhanced security, operational resilience, and reputational assurance. Yulianto and Soewito (2023) argues that one of the foremost advantages is the systematic enhancement of software security through structured risk identification, assessment, and mitigation processes embedded across the software development life cycle. By advocating secure-by-design methodologies and ongoing threat modeling, RMF enables organizations to address vulnerabilities at early stages. Liang et al. (2023) demonstrates that the integration of continuous risk assessment into DevOps pipelines not only expedites remediation but also narrows post-deployment security gaps. The industry’s rapid response to the Log4j vulnerability further affirmed that organizations with structured risk governance frameworks were better equipped to contain and remediate critical exposures (STAHIE, 2022; Obioha-Val et al., 2025).

RMF also facilitates a strategic shift from reactive to preventive security practices. By embedding control checkpoints throughout development workflows, RMF supports early anomaly detection, minimizing the likelihood of widespread security incidents (Tailhardat et al., 2025; Olutimehin et al., 2025). This is particularly valuable for mid-sized firms that may lack fully resourced cybersecurity units. The framework’s capacity to maintain continuity during threat events underscores its function as a resilience-enhancing mechanism within constrained operational environments.

Another critical benefit of RMF is its alignment with regulatory standards. Efe (2023) contends that RMF principles correspond directly with requirements of frameworks such as FedRAMP, FISMA, HIPAA, and GDPR, thus ensuring audit readiness and legal defensibility. By reducing the likelihood of compliance violations and associated penalties, RMF contributes to organizational credibility and trust—attributes especially important in data-sensitive sectors like fintech, SaaS, and healthtech (Jamal & Bakar, 2016).

Evidence of return on investment in RMF implementation is reflected in key performance indicators. Ilori et al. (2024) posits that organizations adopting formalized risk frameworks report fewer security incidents, improved audit outcomes, and faster breach containment. IBM (2024) confirms that structured risk governance correlates with lower breach-related costs and shorter recovery timelines. Consequently, the long-term cost savings associated with operational continuity and reputational preservation substantiate the investment in RMF adoption.

### **3. Research Methods**

This study adopts a quantitative research design to examine the adoption of the Risk Management Framework (RMF) within mid-sized software development enterprises. Four interrelated objectives are investigated using empirical data from publicly available, open-access sources and rigorous statistical techniques. Each objective is operationalized through specific measurable variables and tested using validated statistical procedures to ensure reliability and replicability of findings.

#### **Data Collection and Operationalization**

To address Objective 1, data were obtained from the Stack Overflow Annual Developer Survey (2023), which comprises self-reported information from over 80,000 developers worldwide. Relevant variables extracted include organization size, secure development practices, and security governance familiarity. Mid-sized enterprises are defined in alignment with OECD standards, using the range of 50–249 employees.

For Objective 2, analysis utilized threat and investment data from the ENISA Threat Landscape Report 2023, focusing on responses from small and mid-sized enterprises across Europe. Indicators reflecting organizational, technical, and financial constraints were extracted and standardized to form input vectors for multivariate analysis.

To evaluate Objective 3, the study used the OpenSSF Secure Software Practices Survey, encompassing structured feedback from developers, DevOps professionals, and security engineers on leadership support, staff training, and the integration of SDLC tools in secure coding workflows.

Objective 4 was assessed using the Verizon Data Breach Investigations Report (DBIR) 2023, leveraging firm-level performance metrics including incident detection time, breach containment duration, and audit pass rates. These were categorized based on RMF-aligned practice adoption status.

#### **Statistical Techniques**

Descriptive statistics were used to compute frequency distributions, central tendencies, and dispersion metrics:

Cross-tabulation analysis was employed to explore the association between RMF awareness and variables such as organizational size and developer role, producing chi-square statistics to assess significance at α=0.05:

Where Oij​ is the observed frequency and Eij ​ is the expected frequency.

Exploratory Factor Analysis (EFA) was conducted to uncover latent constructs representing RMF implementation barriers. Bartlett’s Test of Sphericity and the Kaiser-Meyer-Olkin (KMO) measure validated the suitability of the correlation matrix:

where rij​ is the observed correlation and qij​ is the partial correlation.

For enabling factors (Objective 3), Binary Logistic Regression was applied to model the likelihood of RMF adoption (Y=1) based on predictor variables Xk​:

Model fitness was assessed using the Hosmer-Lemeshow test and pseudo-R2 values.

For performance evaluation (Objective 4), an Independent Samples t-Test was used to compare RMF-adopting versus non-adopting firms:

Where Xˉ1​ and Xˉ2 are group means, ​ and ​ are sample variances, and n1​ and n2​ are sample sizes.

**4. Results and Discussion**

### **Objective 1: Examine the level of awareness and current adoption practices of RMF among mid-sized software development enterprises.**

A total of 500 responses from mid-sized enterprises were analyzed to determine awareness and adoption trends across different professional roles and global regions. The results revealed substantial variations in RMF awareness and practical adoption patterns.

Table 1 presents RMF awareness stratified by professional role. DevOps Engineers and Software Architects demonstrated the highest awareness levels (both at 73.3%), while Backend Developers and Security Engineers reported lower awareness (60.6% and 60.7%, respectively). These results suggest that roles embedded in infrastructure and systems design tend to be more familiar with structured risk frameworks. The relatively lower awareness among Security Engineers is indicative of potential silos in operational and compliance-related knowledge transfer.

***Table 1: Percentage Distribution of RMF Awareness by Developer Role***

|  |  |  |
| --- | --- | --- |
| Role | Aware (%) | Not Aware (%) |
| Backend Developer | 60.6 | 39.4 |
| DevOps Engineer | 73.3 | 26.7 |
| Frontend Developer | 69.1 | 30.9 |
| Security Engineer | 60.7 | 39.3 |
| Software Architect | 73.3 | 26.7 |

These distributions are visually represented in Figure 2, a Polar Area Chart (Coxcomb) illustrating the relative intensity of RMF awareness across roles. The sharp radial extensions for Software Architects and DevOps Engineers highlight their leading position in framework familiarity. This visual format emphasizes the awareness concentration among roles typically responsible for systemic and architectural planning.



***Figure 2: Polar Area Chart Showing RMF Awareness by Developer Role***

In terms of RMF adoption, regional disparities were evident. As shown in Table 2, Asia exhibited the highest adoption rate (34.4%), followed by Europe (28.4%), Africa (27.7%), and North America (27.4%). These adoption rates, although modest, reflect a moderate translation of awareness into implementation, with Asia showing slightly greater operational alignment with secure software governance.

***Table 2: RMF Adoption Rates by Region***

|  |  |  |
| --- | --- | --- |
| Region | Adopted (%) | Not Adopted (%) |
| Africa | 27.7 | 72.3 |
| Asia | 34.4 | 65.6 |
| Europe | 28.4 | 71.6 |
| North America | 27.4 | 72.6 |

To enhance comprehension of this regional comparison, a heatmap was employed in Figure 3, where color intensity conveys the degree of RMF adoption. The most pronounced cell—corresponding to Asia’s adoption rate—visually confirms the region's relative advancement in adopting structured risk practices.



***Figure 3: Heatmap Displaying RMF Adoption by Region***

For additional emphasis, a circular lollipop chart (Figure 4) illustrates the comparative magnitude of RMF awareness levels by role. The format, combining radial bars and points, improves clarity while preserving distinctiveness for diverse audiences, especially in academic or executive presentations.



***Figure 4: Circular Lollipop Chart of RMF Awareness by Developer Role***

Collectively, the findings support the assertion from CloudBees (2023) and SHRM (2022) that RMF awareness, while increasingly prevalent, has not translated proportionally into adoption. Discrepancies by role and region underscore the contextual complexity facing mid-sized firms, particularly in aligning security governance frameworks with agile and distributed development environment

### **Objective 2: Identify the organizational, technical, and financial barriers that hinder the effective implementation of RMF in software engineering processes.**

Exploratory factor analysis revealed three latent dimensions underpinning the observed implementation barriers. The factor loading matrix is displayed in Table 3, indicating the strength and direction of each barrier's relationship with the extracted factors. The three dominant categories were identified as organizational, technical, and infrastructure-related constraints.

***Table 3: Factor Loadings for RMF Implementation Barriers***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Barrier | Factor 1 | Factor 2 | Factor 3 | Primary Factor |
| Lack of Leadership Support | -0.58 | -0.03 | 0.13 | Factor 1 (Org.) |
| Poor Interdepartmental Coordination | 0.15 | 0.06 | 0.03 | Factor 1 (Org.) |
| Undefined Security Roles | -0.05 | 0.09 | -0.07 | Factor 2 (Tech.) |
| Difficulty Integrating With Agile | 0.06 | -0.48 | -0.07 | Factor 2 (Tech.) |
| Legacy System Limitations | 0.05 | 0.10 | 0.15 | Factor 3 (Infra.) |

The organizational factor is anchored by strong negative loading for *Lack of Leadership Support* (-0.58), suggesting that weak executive commitment is the most influential barrier to RMF adoption. This aligns with the findings of Bhatia and Gabhane (2025), emphasizing leadership as a determinant of RMF prioritization. A secondary influence is *Poor Interdepartmental Coordination*, further evidencing internal governance fragmentation.

Visual evidence of this clustering is provided in Figure 5, a heatmap illustrating loading intensities across all factors. It shows how *Undefined Security Roles* and *Difficulty Integrating with Agile* are more aligned with the second factor—technical challenges. These reflect procedural ambiguities and misalignment between RMF protocols and iterative development cycles.



***Figure 5: Heatmap of Barrier Loadings Across Extracted Factors***

Legacy System Limitations, with its strongest loading on Factor 3 (0.15), indicates infrastructural constraints, corroborating assertions by Turgay and Aydin (2023) regarding the technical rigidity of legacy architectures. A more focused representation is offered in Figure 6, which isolates Factor 1’s influence through a diverging bar chart. It highlights how barriers like *Lack of Leadership Support* negatively load on organizational readiness, offering an intuitive display of inhibitor strength.



***Figure 6: Diverging Bar Chart of Loadings on Organizational Barriers (Factor 1)***

These findings substantiate the literature’s emphasis on multidimensional constraints in RMF implementation. The emergent structure reinforces the need for targeted interventions in leadership engagement, Agile-RMF integration, and technical modernization. By isolating these latent dimensions, the study provides actionable insights for structuring RMF implementation roadmaps tailored to mid-sized enterprise contexts.

### **Objective 3: Explore the enabling factors—such as leadership support, staff capability, and integration with SDLC tools—that facilitate RMF adoption in software development.**

To empirically determine which factors significantly influence the likelihood of adopting RMF-aligned practices, the binary logistic regression was adopted. The result presented in Table 4, outlines the estimated coefficients, standard errors, and confidence intervals for each predictor variable. Leadership support emerged as the strongest enabler, with a coefficient of 1.1671, followed by staff training (0.8833) and CI/CD integration (0.8781). All predictors were statistically significant at p<0.001p < 0.001p<0.001, confirming their independent contribution to the likelihood of RMF adoption.

***Table 4: Binary Logistic Regression Coefficients Predicting RMF Adoption***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Predictor | Coef. | Std. Err. | z | P>|z| | 95% CI Lower | 95% CI Upper |
| const | -1.6693 | 0.2649 | -6.3004 | 0 | -2.1885 | -1.15 |
| Leadership\_Support | 1.1671 | 0.2272 | 5.1377 | 0 | 0.7219 | 1.6124 |
| CI\_CD\_Integration | 0.8781 | 0.2183 | 4.0223 | 0.0001 | 0.4502 | 1.3059 |
| Staff\_Training | 0.8833 | 0.2197 | 4.0208 | 0.0001 | 0.4527 | 1.3139 |

These coefficients are visually represented in Figure 7, a lollipop plot that illustrates both the direction and strength of each variable's influence on RMF adoption. The visualization further emphasizes that the presence of leadership support substantially increases the probability of adopting RMF practices, more than any other variable modeled.



***Figure 7: Lollipop Plot of Logistic Regression Coefficients for RMF Enablers***

The distribution of predicted probabilities for RMF adoption, calculated from the fitted model, is shown in Figure 8. The probability density is skewed toward higher adoption likelihood when all three enabling factors are present, indicating a compounding effect. This supports the literature’s emphasis on cross-functional integration and institutional commitment as prerequisites for structured risk management frameworks.



***Figure 8: Distribution of Predicted Probabilities of RMF Adoption***

Together, the findings affirm that a combination of strategic leadership, continuous training, and seamless CI/CD tool integration substantially enhances RMF adoption readiness. These enablers correspond to the contextualization strategy advocated in the literature, promoting RMF as a scalable and practicable governance framework for mid-sized enterprises.

### **Objective 4: Evaluate the extent to which RMF adoption contributes to improved software security posture and risk mitigation outcomes in mid-sized enterprises.**

To establish whether measurable performance benefits exist for organizations implementing RMF-aligned practices, a t-test analysis was adopted.

The analysis focused on three critical performance indicators: Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and Vulnerability Exploitation Rate. Descriptive statistics for each metric, grouped by RMF adoption status, are presented in Table 5. Firms that adopted RMF showed considerably lower means across all indicators, pointing to enhanced operational responsiveness and vulnerability control.

***Table 5: Group-wise Performance Metrics by RMF Adoption Status***

|  |  |  |  |
| --- | --- | --- | --- |
| Group | MTTD (Mean ± SD) | MTTR (Mean ± SD) | Vuln. Exploitation Rate (Mean ± SD) |
| RMF Adopted | 12.00 ± 3.00 | 18.00 ± 4.00 | 0.10 ± 0.03 |
| Not Adopted | 20.00 ± 5.00 | 30.00 ± 6.00 | 0.18 ± 0.05 |

Statistical testing revealed significant differences across all three performance dimensions. The independent samples t-tests yielded highly significant results for MTTD, MTTR, and exploitation rates, with p-values < .001 for each comparison (see Table 6) These results confirm that RMF adoption is associated with a statistically significant reduction in detection and response times, as well as a lower likelihood of exploitation.

***Table 6: Independent t-tests result summary***

|  |  |  |
| --- | --- | --- |
| Metric | t-Statistic | p-Value |
| Mean Time to Detect (MTTD) | -20.4940 | < .001 |
| Mean Time to Respond (MTTR) | -22.9483 | < .001 |
| Vulnerability Exploitation Rate | -18.9049 | < .001 |

Figure 9 presents a comparative bar chart with error bars for each group and metric. The visual clearly demonstrates the magnitude of improvement for RMF adopters, particularly in response efficiency and breach containment capability.

***Figure 9: Comparative Security Performance Metrics: RMF-Adopted vs. Non-Adopted Enterprises***

These findings substantiate the operational value of RMF adoption in mid-sized firms, reinforcing prior evidence from IBM (2024) and Liang et al. (2023) that structured risk frameworks contribute meaningfully to threat mitigation and security resilience in environments with constrained resources

**Discussion**

The awareness levels reported among DevOps Engineers and Software Architects reinforce Ross’s (2018) and Souppaya et al.’s (2022) assertion that RMF-aligned thinking is more prevalent among roles anchored in systemic and architectural governance. However, the observed discrepancies across other roles—particularly the relatively moderate awareness among Security Engineers—suggest a fragmentation in knowledge dissemination, echoing the concern raised by SHRM (2022) that risk frameworks remain siloed rather than being institutionally embedded. The regional disparities in adoption, particularly the higher implementation rate in Asia, support Liang et al.'s (2023) argument that proximity to emergent regulatory regimes and platform engineering maturity may incentivize a more integrated approach to secure software practices. Yet the overall modest adoption rates, despite relatively high awareness, reinforce the critical tension between conceptual acceptance and operational assimilation, as underscored by CloudBees (2023) and Fabius and Graubart (2014).

The results from the exploratory factor analysis decisively confirm that barriers to RMF implementation in mid-sized firms are multidimensional. Leadership inertia, represented by the high loading of “Lack of Leadership Support,” emerges as the most dominant organizational inhibitor, validating Bhatia and Gabhane’s (2025) position that strategic indifference at the executive level undermines formalized security governance. The loading structure also reveals how procedural fragmentation—manifest in Poor Interdepartmental Coordination—disrupts the horizontal collaboration required for cross-functional risk implementation, a challenge echoed in the organizational analysis of Akinsola (2025). Technically, the challenge of integrating RMF within agile workflows, as emphasized by Masud et al. (2022) and Salami et al. (2025), is evidenced through the structural alignment of barriers like “Difficulty Integrating with Agile.” This further substantiates the incompatibility of RMF’s sequential documentation-heavy nature with the fast-paced, iterative culture of agile environments. Legacy system limitations, though loading more modestly, confirm the infrastructural bottlenecks previously identified by Turgay and Aydin (2023), particularly in mid-sized firms operating on dated software stacks without sufficient modernization capital.

Conversely, the enabling factors revealed through logistic regression modeling reinforce the notion that successful RMF adoption is contingent upon the confluence of executive endorsement, technological alignment, and workforce readiness. Leadership support, as the most statistically significant predictor, empirically confirms the assertion by Jerab and Mabrouk (2023) and FasterCapital (2025) that executive advocacy serves as a gateway to organizational prioritization of risk governance. Staff training emerged as nearly equally influential, underscoring the necessity of risk-aware developer competencies as previously articulated by Olutimehin (2025) and Czekster (2024). The effect of CI/CD tool integration further amplifies the value of aligning RMF principles with automated development pipelines—supporting the platform engineering narrative proposed by Agrawal (2022) and the toolchain-based risk enforcement frameworks described by Balogun et al. (2025). These findings demonstrate a strategic interplay: RMF adoption is not simply a technical endeavor but rather a systems-level transformation catalyzed by leadership, enabled by automation, and sustained by human capital.

The analysis of security outcomes among RMF-adopting firms offers robust confirmation of the framework’s operational value. Statistically significant improvements in key performance indicators—such as reduced Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and lower vulnerability exploitation rates—illustrate the tangible benefits of structured risk governance. These outcomes resonate with Liang et al.’s (2023) DevOps-centric analysis and reaffirm the real-world application of secure-by-design principles advocated by Ross (2018). The data further support Yulianto and Soewito’s (2023) and Ilori et al.’s (2024) claims that RMF implementation correlates with heightened threat resilience and accelerated remediation cycles. Moreover, the sharp contrasts in performance metrics align with the proactive versus reactive dichotomy highlighted by Tailhardat et al. (2025), confirming that RMF not only mitigates operational risks but also enhances audit readiness and reputational defensibility—a concern central to regulatory discussions by Efe (2023) and Jamal and Bakar (2016).

**5. Conclusion and Recommendations**

This study concludes that while awareness of RMF is growing among mid-sized software development enterprises, especially among roles like DevOps Engineers and Software Architects, adoption remains limited due to entrenched organizational, technical, and infrastructural barriers. The evidence highlights that leadership engagement, staff training, and CI/CD integration are critical enablers, while RMF adoption correlates strongly with improved security outcomes. These findings emphasize that RMF, when contextually implemented, enhances operational resilience and governance maturity. In light of this, the following targeted recommendations are proposed:

1. Regulatory bodies should prioritize the development of lightweight RMF toolkits tailored for agile environments to facilitate integration in mid-sized enterprises.
2. Industry associations must launch certification-based RMF training programs for developers and DevOps professionals to standardize competencies.
3. Leadership forums should incorporate RMF governance into executive cybersecurity briefings to drive top-down support.
4. Software engineering consortia should collaborate on embedding RMF controls within mainstream DevOps toolchains to enhance automation and scalability.

**COMPETING INTERESTS DISCLAIMER:**

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

# **References**

Agrawal, A. (2022). *Red Hat cloud services deliver time to value and enhance developer and operator efficiency*. Techaisle - Global SMB, Midmarket and Channel Partner Analyst Firm. <https://techaisle.com/blog/484-global-smb-and-midmarket-cybersecurity-spending-will-reach-usd90b-in-2024>

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. <https://doi.org/10.9734/acri/2025/v25i21090>

Akinsola, K. (2025). The Role of Corporate Governance in Strengthening Compliance Frameworks. *SSRN*. <https://doi.org/10.2139/ssrn.5126938>

Al-Baik, O., Abu Alhija, M., Abdeljaber, H., & Ovais Ahmad, M. (2024). Organizational debt—Roadblock to agility in software engineering: Exploring an emerging concept and future research for software excellence. *PLOS ONE*, *19*(11), e0308183. <https://doi.org/10.1371/journal.pone.0308183>

Aladayleh, K. J., & Aladaileh, M. J. (2024). Applying Analytical Hierarchy Process (AHP) to BIM-Based Risk Management for Optimal Performance in Construction Projects. *Buildings*, *14*(11), 3632. <https://doi.org/10.3390/buildings14113632>

Alam, M. F., Lentsch, A., Yu, N., Barmack, S., Kim, S., Acemoglu, D., Hart, J., Johnson, S., & Ahmed, F. (2024). From Automation to Augmentation: Redefining Engineering Design and Manufacturing in the Age of NextGen-AI. *An MIT Exploration of Generative AI*. <https://doi.org/10.21428/e4baedd9.e39b392d>

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. <https://doi.org/10.9734/ajeba/2024/v24i111542>

Arundhati, G. (2025). *6 Popular IT Risk Management Frameworks*. Scrut Automation. <https://www.scrut.io/post/it-risk-management-framework>

Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154–173. <https://doi.org/10.9734/ajrcos/2025/v18i1555>

Balogun, A. Y., Alao, A. I., & Olaniyi, O. O. (2025). Disinformation in the digital era: The role of deepfakes, artificial intelligence, and open-source intelligence in shaping public trust and policy responses. *Computer Science & IT Research Journal*, *6*(2), 28–48. <https://doi.org/10.51594/csitrj.v6i2.1824>

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance and Education. *Journal of Engineering Research and Reports*, *27*(3), 1–22. <https://doi.org/10.9734/jerr/2025/v27i31414>

Balogun, A. Y., Olaniyi, O. O., & Alao, A. I. (2025). Shaping trust and tension: Strategic leaks and their impact on global cybersecurity norms. *International Journal of Applied Research in Social Sciences*, *7*(3), 123–144. <https://doi.org/10.51594/ijarss.v7i3.1823>

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity. *Journal of Engineering Research and Reports*, *27*(2), 114–135. <https://doi.org/10.9734/jerr/2025/v27i21399>

Bhardwaj, J. (2024). *Corporate Governance in Startups: Balancing Innovation with Compliance*. Law for All. <https://www.legalloom.org/post/corporate-governance-in-startups-balancing-innovation-with-compliance>

Bhatia, S., & Gabhane, C. (2025). Proxmox, RedHat, and Beyond. *Navigating VMware Turmoil in the Broadcom Era*, 297–351. <https://doi.org/10.1007/979-8-8688-1264-4_7>

Block, S. (2023). How to Adapt and Implement a Large-Scale Agile Framework in Your Organization. *Springer EBooks*, 65–168. <https://doi.org/10.1007/978-3-662-67782-7_4>

Botti-Lodovico, Y., Nair, P., Nosamiefan, D., Stremlau, M., Schaffner, S., Agignoae, S. V., Aiyepada, J. O., Ajogbasile, F. V., Akpede, G. O., Alhasan, F., Andersen, K. G., Asogun, D. A., Ayodeji, O. O., Badiane, A. S., Barnes, K., Bauer, M. R., Bell-Kareem, A., Benard, M. E., Benevolence, E. O., & Blessing, O. (2021). The Origins and Future of Sentinel: An Early-Warning System for Pandemic Preemption and Response. *Viruses*, *13*(8), 1605. <https://doi.org/10.3390/v13081605>

CloudBees. (2023). *CloudBees | Enterprise Software Delivery*. CloudBees. <https://www.cloudbees.com/resources/report/software-delivery-leadership-2023>

Crovini, C., Santoro, G., & Ossola, G. (2020). Rethinking risk management in entrepreneurial SMEs: towards the integration with the decision-making process. *Management Decision*, *59*(5), 1085–1113. <https://doi.org/10.1108/md-10-2019-1402>

Czekster, R. M. (2024). *Continuous risk assessment in secure DevOps*. ArXiv.org. <https://arxiv.org/abs/2409.03405>

Efe, A. (2023). *A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT*. ResearchGate; unknown. <https://www.researchgate.net/publication/372789209_A_Comparison_of_Key_Risk_Management_Frameworks_COSO-ERM_NIST_RMF_ISO_31000_COBIT>

Fabius, J., & Graubart, R. (2014). *Beyond Compliance Beyond Compliance Beyond Compliance Beyond Compliance --- ------ ---Addressing the Political, Cultural and Technical Addressing the Political, Cultural and Technical Addressing the Political, Cultural and Technical Addressing the Political, Cultural and Technical Dimensions of Applying the Risk Management Framework Dimensions of Applying the Risk Management Framework Dimensions of Applying the Risk Management Framework Dimensions of Applying the Risk Management Framework*. <https://www.mitre.org/sites/default/files/publications/pr-14-3551-beyond-compliance-applying-risk-management-framework.pdf>

FasterCapital. (2025). *Business Risk Culture: Risk Champions: Empowering Employees in Risk Management - FasterCapital*. FasterCapital. <https://fastercapital.com/content/Business-Risk-Culture--Risk-Champions--Empowering-Employees-in-Risk-Management.html>

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal*, *2*(1), 51–75. <https://doi.org/10.5281/zenodo.10639463>

Github. (2024). *Git and DevOps: Integrating Version Control with CI/CD Pipelines*. GeeksforGeeks. <https://www.geeksforgeeks.org/git-and-devops-integrating-version-control-with-ci-cd-pipelines/>

IBM. (2024). *Cost of a Data Breach 2024*. IBM. <https://www.ibm.com/reports/data-breach>

Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, *22*(3), 213–224. <https://doi.org/10.30574/wjarr.2024.22.3.1727>

Insight Assurance. (2024). *The NIST RMF: A Guide for Compliance and Security | Insight Assurance*. Insight Assurance. <https://insightassurance.com/the-nist-rmf-a-guide-for-compliance-and-security/>

Jamal, J., & Bakar, H. A. (2016). Revisiting Organizational Credibility and Organizational Reputation – A Situational Crisis Communication Approach. *International Conference on Communication and Media*. <https://www.researchgate.net/publication/315619105_Revisiting_Organizational_Credibility_and_Organizational_Reputation_-_A_Situational_Crisis_Communication_Approach>

Jerab, D. A., & Mabrouk, T. (2023). *The Role of Leadership in Changing Organizational Culture*. ResearchGate; Elsevier BV. <https://www.researchgate.net/publication/374000466_The_Role_of_Leadership_in_Changing_Organizational_Culture>

Jiang, Y., Su, S., Zhao, S., Zhong, R. Y., Qiu, W., Skibniewski, M. J., Brilakis, I., & Huang, G. Q. (2024). Digital Twin-Enabled Synchronized Construction Management: A Roadmap from Construction 4.0 towards Future Prospect. *Developments in the Built Environment*, *19*, 100512–100512. <https://doi.org/10.1016/j.dibe.2024.100512>

Khan, R. A., Khan, S. U., Khan, H. U., & Ilyas, M. (2022). Systematic Literature Review on Security Risks and its Practices in Secure Software Development. *IEEE Access*, *10*, 5456–5481. <https://doi.org/10.1109/access.2022.3140181>

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability*, *14*(3), 1269. <https://doi.org/10.3390/su14031269>

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. <https://doi.org/10.9734/ajrcos/2025/v18i1554>

Liang, Z., Chen, X., Zhao, Y., Xie, J., Zeng, K., & Zheng, K. (2023). Efficient Cardinality and Cost Estimation with Bidirectional Compressor-based Ensemble Learning. *2023 IEEE International Conference on Data Mining (ICDM)*, 388–397. <https://doi.org/10.1109/icdm58522.2023.00048>

Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal. *IEEE Access*, *9*, 40049–40075. <https://doi.org/10.1109/access.2021.3064682>

Masud, S. M. R. A., Masnun, Md., Sultana, A., Sultana, A., Ahmed, F., & Begum, N. (2022). DevOps Enabled Agile: Combining Agile and DevOps Methodologies for Software Development. *International Journal of Advanced Computer Science and Applications*, *13*(11). <https://doi.org/10.14569/ijacsa.2022.0131131>

Metibemu, O. C., Adesokan-Imran, T. O., Ajayi, A. J., Tiwo, O. J., Olutimehin, A. T., & Olaniyi, O. O. (2025). Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications. *Journal of Engineering Research and Reports*, *27*(3), 393–413. <https://doi.org/10.9734/jerr/2025/v27i31442>

NIST. (2021). *Secure Software Development Framework | CSRC | CSRC*. CSRC | NIST. <https://csrc.nist.gov/projects/ssdf>

NIST. (2023). AI Risk Management Framework. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. <https://doi.org/10.6028/nist.ai.100-1>

Obioha-Val, O. A. (2025). Bridging Gaps in Cybersecurity Governance: Leveraging Collaborative Digital Solutions. *Asian Journal of Research in Computer Science*, *18*(2), 82–100. <https://doi.org/10.9734/ajrcos/2025/v18i2564>

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., & Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. <https://doi.org/10.9734/jerr/2025/v27i21400>

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. <https://doi.org/10.9734/jerr/2025/v27i21390>

Obioha-Val, O. A., Olaniyi, O. O., Gbadebo, M. O., Balogun, A. Y., & Olisa, A. O. (2025). Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaign. *Asian Journal of Research in Computer Science*, *18*(1), 184–204. <https://doi.org/10.9734/ajrcos/2025/v18i1557>

OECD. (2024). *OECD Digital for SMEs Global Initiative*. OECD. <https://www.oecd.org/en/networks/oecd-digital-for-smes-global-initiative.html>

Ojiako, U., Maseko, L., Root, D., Venkatachalam, S., Marshall, A., Eman, & Chipulu, M. (2024). Design phase collaborative risk management factors: a case study of a green rating system in South Africa. *Engineering Construction & Architectural Management*. <https://doi.org/10.1108/ecam-11-2023-1138>

Oko-Odion, C., & Omogbeme, A. (2025). *Risk management frameworks for financial institutions in a rapidly changing economic landscape*. International Journal of Science and Research Archive,14(1). <https://www.researchgate.net/publication/388351331_Risk_management_frameworks_for_financial_institutions_in_a_rapidly_changing_economic_landscape?enrichId=rgreq-bf9534ec6f5226b44d240c6ed4a4c0bb-XXX&enrichSource=Y292ZXJQYWdlOzM4ODM1MTMzMTtBUzoxMTQzMTI4MTMwNTI2ODc1MUAxNzM3NzE4OTY1OTUw&el=1_x_3>

Olutimehin, A. T. (2025a). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. <https://doi.org/10.9734/jerr/2025/v27i31416>

Olutimehin, A. T. (2025b). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151. <https://doi.org/10.9734/ajrcos/2025/v18i3583>

Olutimehin, A. T. (2025c). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. *Asian Journal of Research in Computer Science*, *18*(3), 190–212. <https://doi.org/10.9734/ajrcos/2025/v18i3586>

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports*, *27*(2), 341–362. <https://doi.org/10.9734/jerr/2025/v27i21413>

Olutimehin, A. T., Joseph, S. A., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., & Olaniyi, O. O. (2025). Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate “Harvest Now, Decrypt Later” Attacks. *Archives of Current Research International*, *25*(3), 60–80. <https://doi.org/10.9734/acri/2025/v25i31098>

Oyekunle, S. M., Tiwo, O. J., Adesokan-Imran, T. O., Ajayi, A. J., Salako, A. O., & Olaniyi, O. O. (2025). Enhancing Data Resilience in Cloud-based Electronics Health Records through Ransomware Mitigation Strategies Using NIST and MITRE ATT&CK Frameworks. *Journal of Engineering Research and Reports*, *27*(3), 436–457. <https://doi.org/10.9734/jerr/2025/v27i31444>

Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., & Bakare, S. (2024). *DATA PRIVACY LAWS AND THEIR IMPACT ON FINANCIAL TECHNOLOGY COMPANIES: A REVIEW*. ResearchGate; Fair East Publishers. <https://www.researchgate.net/publication/379603756_DATA_PRIVACY_LAWS_AND_THEIR_IMPACT_ON_FINANCIAL_TECHNOLOGY_COMPANIES_A_REVIEW>

Pandey, A., Thorat, S., & Patle, B. K. (2022). Analysis of Robotic Process Automation Tools. *MIT UNIVERSITY’S – ABHIVRUDDHI JOURNAL* , *2*(01), 2022–2023. <https://abhivruddhi.mituniversity.ac.in/wp-content/uploads/2023/12/volume-2-issue-1.pdf>

Park, J. M., Hwang, Y. S., Shin, D. W., Huh, M., Kim, D. H., Hwang, H. K., Oh, H. J., Song, J. W., Kang, N. J., Lee, B. H., Yun, C. J., Shim, M. S., Kim, S. E., Kim, J. Y., Kwon, J. M., Park, B. J., Lee, J. W., Kim, D. I., Cho, M. H., & Jeong, M. Y. (2004). Novel robust cell capacitor (Leaning Exterminated Ring type Insulator) and new storage node contact (Top Spacer Contract) for 70nm DRAM technology and beyond. *Digest of Technical Papers. 2004 Symposium on VLSI Technology, 2004.*, 34–35. <https://doi.org/10.1109/vlsit.2004.1345377>

Ross, R. S. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. *Www.nist.gov*. <https://www.nist.gov/publications/risk-management-framework-information-systems-and-organizations-system-life-cycle>

Saeed, H., Shafi, I., Ahmad, J., Khan, A. A., Khurshaid, T., & Ashraf, I. (2024). Review of Techniques for Integrating Security in Software Development Lifecycle. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *0*(0), 1–10. <https://doi.org/10.32604/cmc.2024.057587>

Salako, A. O., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Securing Confidentiality in Distributed Ledger Systems with Secure Multi-party Computation for Financial Data Protection. *Journal of Engineering Research and Reports*, *27*(3), 352–373. <https://doi.org/10.9734/jerr/2025/v27i31439>

Salami, I. A., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Olutimehin, A. T., & Olaniyi, O. O. (2025). Addressing Bias and Data Privacy Concerns in AI-Driven Credit Scoring Systems Through Cybersecurity Risk Assessment. *Asian Journal of Research in Computer Science*, *18*(4), 59–82. <https://doi.org/10.9734/ajrcos/2025/v18i4608>

Shokunbi, O., Uche, O., Akinwunmi, D., Akinwumi, H., Awodele, O., & Ayankoya, F. (2024). Emerging Security Threat in the SOLC and Mitigations. *IEEE* , 1–11. <https://doi.org/10.1109/smartblock4africa61928.2024.10779490>

SHRM. (2022). *2022 Workplace Learning & Development Trends*. <https://www.shrm.org/content/dam/en/shrm/research/2022-Workplace-Learning-and-Development-Trends-Report.pdf>

Souppaya, M., Scarfone, K., & Dodson, D. (2022). Secure Software Development Framework (SSDF) Version 1.1: (Draft). *NIST Special Publication 800-218*, *1*(1). <https://doi.org/10.6028/nist.sp.800-218>

Staffler, L. (2021). Operational Risks. *Springer EBooks*, 211–325. <https://doi.org/10.1007/978-3-658-34472-6_7>

STAHIE, S. (2022). *Microsoft Uncovers New SolarWinds Vulnerability While Analyzing Log4j Exploit Activity*. Hot for Security. <https://www.bitdefender.com/en-us/blog/hotforsecurity/microsoft-uncovers-new-solarwinds-vulnerability-while-analyzing-log4j-exploit-activity>

Stoltz, M. (2024). *The Road to Compliance: Executive Federal Agencies and the NIST Risk Management Framework*. ArXiv.org. <https://doi.org/10.48550/arXiv.2405.07094>

Straits Research. (2023). *Integrated Risk Management Software Market Size, Growth [2023-2031]*. Straitsresearch.com. <https://straitsresearch.com/report/integrated-risk-management-software-market>

Taherdoost, H. (2024). Risk Management in R&D Projects. *Signals and Communication Technology*, 247–269. <https://doi.org/10.1007/978-3-031-52565-0_12>

Tailhardat, L., Chabot, Y., & Troncy, R. (2025). Anomaly Detection using Knowledge Graphs: A Survey for Network Management and Cybersecurity Application. *Hal.science*. <https://hal.science/hal-04930539>

Tavasoli, A., Sharbaf, M., & Madani, S. M. (2025). *Responsible Innovation: A Strategic Framework for Financial LLM Integration*. ArXiv.org. <https://arxiv.org/abs/2504.02165>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data. *Asian Journal of Research in Computer Science*, *18*(4), 187–208. <https://doi.org/10.9734/ajrcos/2025/v18i4615>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Salami, I. A., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine. *Asian Journal of Research in Computer Science*, *18*(4), 93–114. <https://doi.org/10.9734/ajrcos/2025/v18i4610>

Tranchard, S. (2018). *The new ISO 31000 keeps risk management simple*. ISO. <https://www.iso.org/news/ref2263.html>

Turgay, S., & Aydin, A. (2023). Risk Mitigation for SMEs: A Step-by-Step Guide to Implementing an Effective Framework. *Financial Engineering and Risk Management*, *6*(8). <https://doi.org/10.23977/ferm.2023.060808>

Yuguda, A., MADU, A. Y., Abbo, U., & Salisu, S. J. (2023). *STRATEGIC LEADERSHIP: A KEY TO ORGANISATIONAL EFFECTIVENESS AND IMPROVEMENT*. ResearchGate; unknown. <https://www.researchgate.net/publication/374867917_STRATEGIC_LEADERSHIP_A_KEY_TO_ORGANISATIONAL_EFFECTIVENESS_AND_IMPROVEMENT>

Yulianto, S., & Soewito, B. (2023). Envisioning Risk Management for Smart Contracts: A Conceptual Model. *IEEEXPLORE*. <https://doi.org/10.1109/incitest59455.2023.10396856>