Computer Fraud and Security
ISSN (online): 1873-7056

Strategic Planning and Stakeholder Communication for Successful IAM Integration

Neha Asthana

Independent Researcher, USA

Abstract

The decommissioning of legacy identity management systems involves the continual aggregation of enterprise application portfolios into unified IAM platforms. Organizations face technical, governance, and resistance challenges in major IAM consolidation initiatives spanning multi-application, business unit, and organizational domains. Effective planning must account for governance structures, escalation procedures, and stakeholder communication to address low technical aptitude and resistance to centralized identity governance. This article examines governance frameworks, stakeholder engagement strategies, risk mitigation approaches, and change management practices that enable successful IAM platform transitions. Quantitative evidence drawn from enterprise deployments demonstrates that structured governance reduces post-migration stabilization periods from nine months to approximately two months, while intelligent validation eliminates up to 78% of manual reconciliation effort. Phased stakeholder engagement programs addressing IAM knowledge gaps across 100-plus IT professionals yielded measurable improvements in onboarding readiness and access provisioning efficiency. Through structured education, periodic governance checkpoints, and systematic knowledge transfer, IAM migration programs convert operational challenges into sustained improvements in security posture, regulatory compliance, and cloud operational efficiency.

Keywords: Identity and Access Management, Stakeholder Engagement, Enterprise Governance, Cloud Migration, Change Management

1. Introduction

The decommissioning of a legacy identity management solution enabled a complex application migration project to consolidate multiple applications into a unified Identity and Access Management (IAM) solution, achieved through careful planning, governance, and stakeholder engagement to enable the roll-out of the new IAM solution across a range of application portfolios. The redevelopment would enable a consistent approach to manage access rights, authentication, and user provisioning across all enterprise applications. Given that data volumes are expected to exceed 180 zettabytes worldwide by 2025, organizations would need to modernize their identity infrastructure while ensuring business continuity and regulatory compliance [1]. The scale of migrating the enterprise application portfolio meant that proactive identification and mitigation of risks, educating the organizations about the processes, and communication to encourage adoption, were required to remove the barriers to achieving a successful migration.

These considerations become more important when an enterprise undertakes IAM consolidation programs at scale. An analysis of the identity and access management processes of enterprise stakeholders found that 72% of those polled indicated that it takes at least one week for an average employee to obtain access rights to all applications and infrastructure platforms required to perform their job duties [2]. Delays are also exacerbated when application owners must negotiate systems access with both the legacy and target environments as part of a migration effort. One study found that 78% of organizations involve more than one department in defining and managing access to systems. This is compounded when an organization is consolidating platforms, requiring agreement between multiple stakeholders on governance models, role definitions, and entitlement structures [2].

On the security side, long access management cycles can create risk exposure for the enterprise. A survey of 233 companies found that 50% of respondents take three or more days to revoke access to enterprise systems for departing employees. This creates a window during which ex-employees can access corporate systems and data [2]. This issue is further compounded in large-scale migration efforts where migrating enterprise application portfolios require access for departing employees to be

explicitly revoked in both legacy and newly modernized enterprise applications [3]. Likewise, across human resources, sales management, and help desk roles, it is noted that 81% of stakeholders believe they can be partly responsible for issues that occur due to access being incorrectly granted, indicating the need for collaboration beyond security-focused teams [2].

Given these factors, understanding stakeholder concerns became key to migration success, as well as establishing governance structures for identity architecture, application onboarding, and control assurance that define respective roles and decision rights for stakeholders. The first two steps of early stakeholder engagement included the definition of the migration objectives and the capabilities of IAM, with platform demonstrations, and later workshops with application owners and vendor representatives to identify obstacles and risks. Two important obstacles that were identified and addressed were lack of IAM knowledge on the application teams and resistance to abandon decentralized access control.

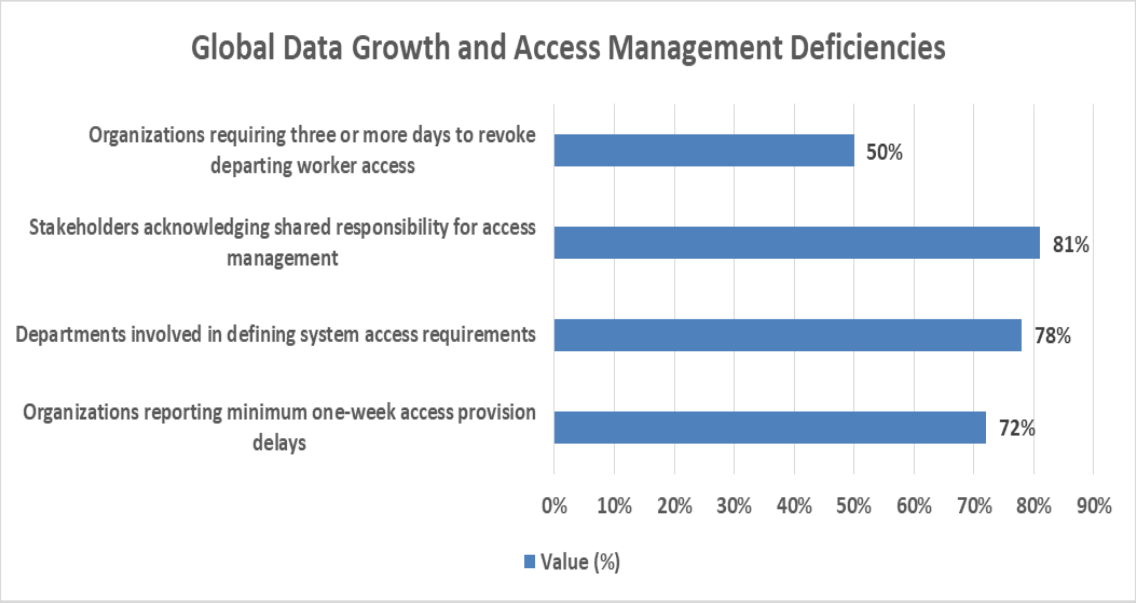

Figure 1: Global Data Growth and Access Management Deficiencies [1, 2]

2. Program Governance and Decision Architecture

A governance framework was formulated to define governance roles and responsibilities that would be accountable for and support the decision-making for the full migration lifecycle: identity architecture review, application onboarding orchestration, and control assurance validation. The technical, operational, and compliance-side roles with their respective decision rights and responsibilities were well represented across the application portfolio. For instance, the identity architecture roles owned the platform configuration standards, connector building patterns, and integration design approvals. The application onboarding coordinators owned the intake workflows, technical readiness assessments, and migration scheduling across the functional domains [3]. Control assurance teams validated segregation of duties policies, entitlement reconciliations, and audit trails for each onboarded application for regulatory compliance throughout the migration program.

The framework included an escalation model, through which any issues that could not be resolved at the working level were escalated through levels of impact and decision complexity. This meant that any blocking issue could be resolved quickly, but governance was put in place around the decision process and oversight for any more broadly impactful organizational decisions, which avoided a governance bottleneck during the migration. Regular governance reviews tracked progress against key milestones, identified emerging risks and changes to scope as business needs evolved, and provided visibility to wave migrations, dependencies being remediated, and the efficient use of resources based on objective metrics rather than subjective business anecdotes [3].

Studying the maturity of existing IAM solutions, this article identifies major gaps in the existing IAM implementations that affect their governance capability during the adoption of platform migration. For a representative set of 10 IAM systems

evaluated in different dimensions, i.e., completeness of functionality, security, privacy, federation, usability, scalability, and efficiency, it is shown that only 36.75 of the 66 points, 55.68%, are covered on average [4]. The current IAM frameworks discussed appear to be insufficient to address rich migration requirements and exhibit weaknesses in certain governance areas such as dynamic access management, improved logging and auditing capabilities, and federated identity management.

However, even the best-performing IAM system only scored 47 of a possible 66 points. Therefore, none of the systems examined offer the entire range of core IAM functionalities required to realize the migration of large enterprises [4]. The underperformance of the worst-scoring decentralized identity management solution (29 out of 66 points) was also related to a lack of consideration of privacy protection, process efficiency, and security properties during platform migration, which must take on greater importance in heterogeneous and multi-technical operational scenarios [4]. The maturity gaps had to be reduced using mitigation controls in the migration program phase, including manual processes, additional security controls, and improved stakeholder engagement processes to reduce the lack of IAM platform functionality.

Regular feedback loops, where application owners and their stakeholders, vendor representatives, and technical teams could raise, address, and escalate concerns through the most appropriate structures, were seen as critical to maintaining stakeholder confidence and program momentum across the multiple phases of the migration program, especially in cases where functional gaps in contemporary IAM systems were being worked around or supplemented with additional controls.

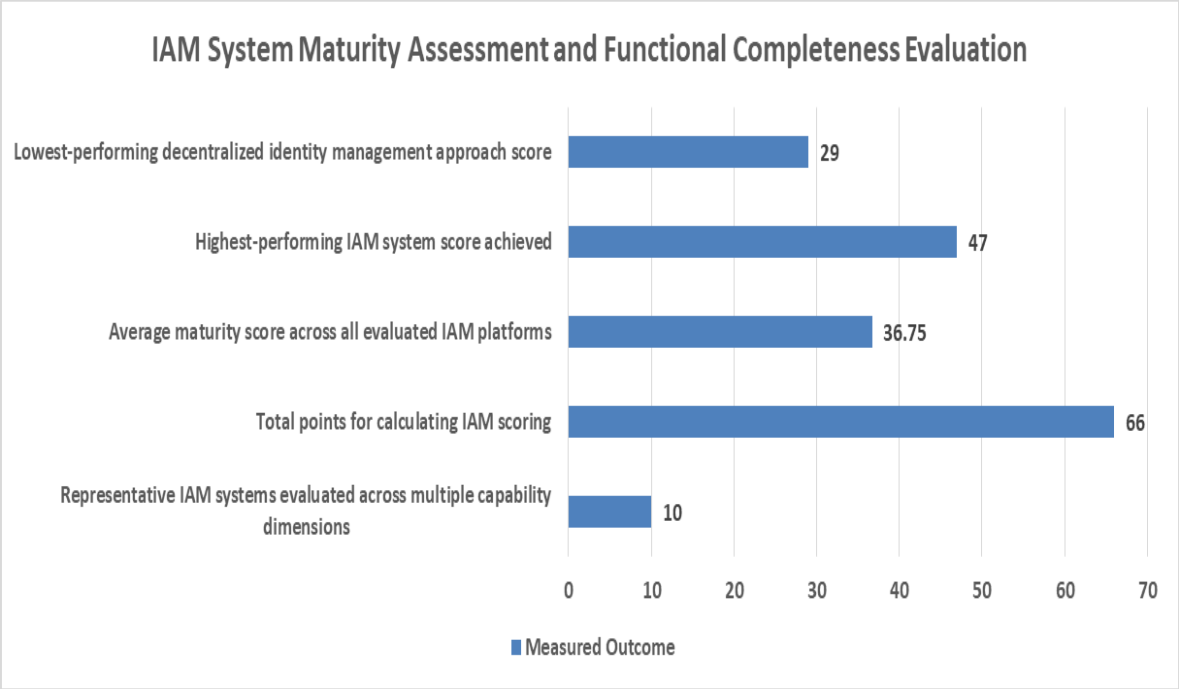

Figure 2: IAM System Maturity Assessment and Functional Completeness Evaluation [3,4]

3. Stakeholder Engagement and Communication Framework

3.1 Structured Engagement Sessions

This first phase was supported by a structured stakeholder engagement approach with meetings and workshops with application owners and technical partner representatives across the application portfolio to communicate plans and timelines, to describe IAM concepts and the platform capabilities, and to show technical capabilities of the platform to address stakeholder challenges. Workshops included architecture overviews for technical stakeholders, compliance benefits for audit and risk stakeholders, and product demonstrations of connectors readied to be used for application owners who needed to see a demonstration to know how a specific connector works [5]. The required follow-up actions and decisions have been

tracked, and accountability has been taken at each of these cross-stakeholder internal meetings to drive the multi-month migration effort.

Stakeholders observed that access delays and access revocations remained an active business operational issue that negatively impacted organizational risk and productivity. Stakeholders also found that the transition to the remote working model exacerbated challenges with timely provisioning of access. Additionally, the stakeholders indicated that the pandemic negatively impacted the execution of customary identity management processes [5]. It was necessary to communicate with stakeholders during the migration project around fears that the service would be taken offline and to ensure that the new platform would not exacerbate any access management issues.

3.2 Tailored Communication Strategy

As the stakeholders shared different goals and technical language, communication was tailored to fit the most relevant topics for each of these contexts. For the infrastructure team that needed to support high-availability environments, it was more relevant to discuss platform availability statistics, disaster recovery procedures, zero-downtime migration approaches, and continuity of service during the migration process. Compliance stakeholders were informed about the audit trail feature, separation of duties, and evidence collection for security assessments and compliance reporting based on principles and practices of zero trust architecture (e.g., continuous authentication, adaptive access control, etc.) [6]. Operations stakeholders were informed about the reduction of workload achieved by automating resource provisioning, implementing a password self-service capability, and decreasing administrative effort associated with manual reconciliation activities.

In common with the broader trend towards zero trust architecture, the IAM platform's position within an enterprise security framework was promoted as a step away from a customary perimeter-based model. A range of messaging focused on the platform's conformance to the "never trust, always verify" model by describing policy engines that continuously evaluated access requests against organizational policies, policy administrators that determined authorization decisions based on those evaluations, and policy enforcement points that enforced access to resources [6]. This architectural description enabled technical stakeholders to understand how the platform would improve their security posture while still providing business agility around dynamic access management.

The findings show that identity management ownership was seen as spanning multiple organizational functions. Stakeholders were aware of weaknesses in existing processes that could be improved and, therefore, volunteered to participate in access governance programs to make identity management more secure and efficient [5]. This also initiated discussions about establishing access governance committees to ease cross-department collaboration between system and data access managers, using a consistent approach, thereby improving the user experience and minimizing audit findings and compliance risk.

Combining IAM's AI-driven capabilities, such as user and entity behavior analytics, with continuous authentication and risk scoring would be able to automatically revoke access privileges, require additional authentication, or trigger an access review when high-risk behavior is detected [6]. The conversations also helped illustrate how these capabilities would alleviate the stakeholder concerns of insider threats and stolen credentials while maintaining user freedom and productivity via adaptive security policies that can increase security without disrupting work across heterogeneous apps and users.

4. Risk Identification and Mitigation

4.1 Identified Deficiencies

The stakeholder engagement sessions identified several major issues to be addressed proactively across the application migration path. For instance, IAM knowledge deficiency within the application teams may impact their onboarding effort. Technical assessments have shown an important portion of the application owner population is unaware of or cannot articulate identity federation protocols, role-based access control (RBAC) models, or entitlement lifecycle concepts. Application owners were often resistant to the adoption, mainly due to concerns over the service interruption, migration effort, and increased operations complexity. Example reasons included concerns over the requirement to retire the local application authentication method, the loss of application-specific administrative privileges, and the disbelief over the benefits of centralized identity governance within the application architecture [7].

An empirical study on migration complexity discusses involving all relevant stakeholders in transformation projects. This study interviewed 12 cloud architects, IT managers, and project leaders in the finance, healthcare, retail, and government sectors. It found similarities in the technical, organizational, and change management hurdles experienced across these sectors [7]. These qualitative measures were supplemented by administering questionnaires to over 100 IT professionals recruited through professional social networks for quantitative measurement of migration outcomes, as well as an opportunity to provide qualitative explanations for their migration challenges. Taken collectively, these measures provide a foundation for understanding the nature of enterprise platform transits and the role of stakeholder perspectives in influencing migration success trajectories across different organizations and industries.

4.2 Mitigation Strategies

Remediation strategies were based on platform configuration and best practice rather than bespoke development or deep configuration with active maintenance overhead. Feedback collated from stakeholders formed a basis for remediation planning. Internal consultation exercises were also conducted with relationship areas, including alumni affairs, internal welfare, extension, planning, teaching, communications, marketing, advanced training, research, and internationalization offices, to ensure a range of organizational perspectives were brought forward during migration strategy development [8]. The terms of this consultation provided an understanding of both technical, operational, and cultural gaps, which could then be addressed with targeted communication, tailored training, and phased implementation according to stakeholder readiness.

The remediation actions included knowledge-building initiatives and alignment of migration actions with institutional sustainability targets. A systematic plan was followed to focus institutional action on the 9 SDGs where the platform had clear capacity to create positive impact as an HEI and where lack of alignment risked failure to achieve institutional aims [8]. Pioneering assessment of contribution towards the SDGs in the priority areas showed how migration governance decisions contributed to meeting 6 out of 13 priority area targets, showing the value-added by migration governance and higher-level institutional commitment beyond a narrow definition of technical modernization [8]. Integrating technical migration planning with SDG frameworks ensured that the migration program furthered rather than weakened calculated priorities and created synergies with the operational transformation. This enabled stakeholders to be confident that the migration program indeed delivered on institutional objectives.

Consultation Component	Coverage Specification
Cloud architects and IT managers interviewed across multiple sectors	12 professionals
IT professionals surveyed through professional networks	Over 100
Sustainable Development Goals prioritized by institution (out of 17)	9
Defined targets directly supported in critical areas (out of 13)	6

Table 1: Stakeholder Consultation and Sustainable Development Goals Integration Strategy [7, 8]

5. Change Management and Knowledge Transfer

Enterprise IAM migration programs can be hampered by cultural and organizational factors (i.e., conceiving and adopting different ways of working) and an unwillingness to accept automated governance processes. Academic research into ITSM platform migrations has found as many as 30-45% of migrations are either delayed considerably or have to be re-implemented due to organizational and technical factors, e.g., weak change management and knowledge transfer practices [10]. Legacy IAM processes featured manual provisioning, de-provisioning, and decentralized authentication. These created dependencies requiring change management at both the technical implementation and organizational acceptance levels [11]. Change management moves organizations from manual control and effort to trust that automated, policy-based controls and processes effectively manage user access to required resources using effective communication, training, and visible evidence of operational improvements[12].

Holistic training programs should address capability deficiencies of disparate stakeholder communities, including technical, compliance, and operational staff. Manual reconciliation of two systems takes as much as 80 hours for every 10000 records to check for successful data migration, which is a labor-intensive and error-prone process [10]. Organizations implementing modern IAM frameworks improve employee productivity through automated validation and provisioning workflows, freeing up administrators' time for more calculated initiatives. Role-based training programs can accelerate technology adoption and operational comprehension. Technical stakeholders require training on specific connectors and accompanying policy configuration or workflows. Compliance stakeholders need training on audit and governance mechanisms [13]. Operational stakeholders need training to use these automated workflows and understand how manual tasks are reduced and integrated with other systems, like ticketing systems [9].

The structured migration roadmap defined within six modernization steps leads to better migration outcomes than ad hoc approaches [9]. In a governance-compliant and risk-reduced approach, organizations can be guided through the migration life cycle stepwise: assessment, strategy definition, architecture development, incremental implementation, optimization, and thorough training [14]. By using the framework, 78% of manual reconciliation efforts could be eliminated through clever validation and reconciliation, transforming data quality assurance from manual checking to clever automation [10].

Post-migration stabilization, when the organization continues to improve and document their processes while knowledge transfer takes place, is an important part. Organizations using full change management found stabilization periods were about 2 months, rather than 9 months for those who used traditional stabilization approaches. This helps organizations achieve steady-state operations to support business objectives more quickly [10]. Documenting organizational workflows, custom integrations, and policy decisions helps to institutionalize knowledge in order to reduce the risk of staff change and enables efficient administration [15]. This type of change management and knowledge transfer transforms threat migration into organizational capabilities that increase sustained competitive advantage.

Change Management Metric	Quantified Performance
ITSM migrations experiencing impactful delays or significant rework	30-45%
Average manual reconciliation time per 10000 records	80 hours
Reduction in manual reconciliation effort through intelligent validation	78%
Post-migration stabilization timeline (with change protocols)	2 months

Table 2: ITSM Migration Impact and Change Management Framework Performance Metrics [9, 10]

Conclusion

The consolidation of legacy identity management systems into unified IAM ecosystems represents a strategic transformation rather than a purely technical upgrade. As hybrid cloud environments expand and regulatory expectations intensify, organizations must approach IAM modernization through structured governance, stakeholder alignment, and disciplined risk management frameworks. Technical deployment alone is insufficient without clearly defined decision rights, escalation mechanisms, and sustained organizational engagement. This article demonstrates that governance-centric migration strategies—supported by targeted stakeholder communication, formalized change management practices, and systematic knowledge transfer—significantly improve transition outcomes. Structured programs reduced post-migration stabilization timelines from nine months to approximately two months, and intelligent validation frameworks eliminated up to 78% of manual reconciliation overhead across enterprise deployments. By integrating automated provisioning, continuous authentication, behavioral analytics, and comprehensive audit capabilities, modern IAM platforms enhance security resilience while simultaneously improving operational efficiency and regulatory compliance.

Several limitations merit acknowledgment. The quantitative evidence cited draws from diverse organizational contexts and may not uniformly apply to all enterprise configurations or regulatory environments. The SDG alignment metrics referenced in Section 4 are specific to higher education institutions and require adaptation for commercial or government deployments. Future work should examine longitudinal outcomes of IAM consolidation programs beyond initial stabilization windows,

with particular attention to sustained compliance posture, identity governance maturity progression, and the impact of emerging agentic AI capabilities on automated access decision-making. Controlled comparative evaluations across industry verticals would further validate the governance and communication frameworks presented here. Ultimately, IAM modernization succeeds when treated as an enterprise-wide transformation initiative that aligns technical architecture with institutional governance objectives, and organizations adopting this integrated approach are better positioned to reduce risk exposure, streamline access management, and sustain long-term agility within increasingly complex digital ecosystems.

References

[1] R. Pandipati, "Cloud Migration Strategies for Enterprise Data Platforms: Architectural Patterns and Implementation Roadmaps," World J. Adv. Eng. Technol. Sci., Dec. 2025. Available: https://wjaets.com/sites/default/files/fulltext_pdf/WJAETS-2025-1535.pdf

[2] Dimensional Research, "Identity and Access Management: The Stakeholder Perspective," 2021. Available: https://www.idsalliance.org/wp-content/uploads/2022/06/IAM-Stakeholder-Perspective.pdf

[3] Sara Aboukadri et al., "Machine learning in identity and access management systems: Survey and deep dive," ScienceDirect, 2024. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404824000300

[4] Yiting Wang et al., "A survey on Identity and Access Management for future IoT services," ScienceDirect, Nov. 2025. Available: https://www.sciencedirect.com/science/article/pii/S138912862500684X

[5] J. Smith, "New Research Provides IAM Stakeholder Perspective on Access Challenges," Identity Defined Security Alliance, 2021. Available: https://www.idsalliance.org/blog/new-research-provides-iam-stakeholder-perspective-on-access-challenges/

[6] Sahil Arora and Apoorva Tewari, "Zero trust architecture in IAM with AI integration," IJSRA, 2023. Available: https://ijsra.net/sites/default/files/IJSRA-2023-0163.pdf

[7] Srikanth Nimmagadda, "A Comprehensive Study of Intricacies of Migrating On-Premises Workloads to the Cloud," JISEM, 2024. Available: https://www.jisem-journal.com/download/19_HR-2466.pdf

[8] Ana M. Osorio et al., "Methodology for Stakeholder Prioritization in the Context of Digital Transformation and Society 5.0," MDPI, 2024. Available: https://www.mdpi.com/2071-1050/16/13/5317

[9] Shreekant Rangrej, "Transitioning Legacy Infrastructure into a Future-Ready IAM Environment that Enhances Scalability, Compliance, and Intelligence," Clareus Scientific Science and Engineering, Nov. 2025. Available: https://clareus.org/pdf/csse/CSSE-02-061.pdf

[10] Mahesh Kumar Damarched, "Using Large Language Models to Automate Enterprise ITSM Platform Migrations: Adaptive Learning Framework for Intelligent Data Validation and Anomaly Detection in ITSM Migration," IJISRT, 27th Jan. 2026. Available: https://www.ijisrt.com/assets/upload/files/IJISRT26JAN689.pdf

[11] Quintero, F. A., "Growth-oriented culture within VFX teams: Implications for high-quality effects and simulation innovation," *International Journal of Computational and Experimental Science and Engineering*, 9(4), 2023.

[12] Belhassen, A., "Machine learning for predictive maintenance: Fusing vibration sensor data and thermal imaging to forecast bearing failure," *Sarcouncil Journal of Engineering and Computer Sciences*, 1(3), 9–18, 2022.

[13] Surana, S., "The efficacy of internal controls and audit committees in mitigating financial risk: Perspectives from Indian corporate governance," *Journal of International Crisis and Risk Communication Research*, 8(S10), 377–386, 2025.

[14] Darteh, F. K., "Challenges in revenue and expenditure reporting: Implications for budget management," *Sarcouncil Journal of Entrepreneurship and Business Management*, 2(11), 1–8, 2023.

[15] Ascanio, G. A., "Material performance and longevity in luxury kitchens: Architectural approaches to durability and use," *Journal of International Crisis and Risk Communication Research*, 7(S9), 3575–3584, 2024.