Journal of Information Systems Engineering and Management
2026, 11(2s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Identity and Access Management in Banking: Governance Automation, Privileged Access, and Zero Trust Enablement

Suneel Kumar Rawat
Independent Researcher, USA

ARTICLE INFO

Received: 07 March 2026

Accepted: 25 March 2026

ABSTRACT

Identity and Access Management (IAM) controls have become a fundamental element of an information security architecture used to govern privileged access and identity lifecycle, support compliance, authenticate customers, and analyze behavior in a modern, distributed, and interconnected banking environment. Risk-adaptive privilege management systems use Zero Trust principles to provide dynamic entitlement access to payment and core banking systems based on composite risk scoring, including behavioral profiling, transaction limits, and geographic anomaly recognition; this capability removes standing accounts, effectively shrinking an organization's attack surface. Integrated bi-directionally with the Human Resources Information Systems (HRIS), Automated IGA systems orchestrate Joiner-Mover-Leaver processes, accelerating provisioning procedures and preventing orphaned accounts found in other systems. Entitlement segregation is enforced through preventive policy engines that block conflicting entitlement combinations from being assigned. Automated certification campaigns generate an audit trail to existing compliance regimes such as SOX, PCI DSS, and the GLBA/FFIEC via tamper-obvious chains of custody. Powered by underlying layered authentication mechanisms based on session risk, customer-facing CIAM deployments can also apply behavioral biometrics, device fingerprinting, and liveness detection to find the right balance between frictionless digital experience and security. In high-value trading scenarios, session brokering technologies, UEBA, and AI/ML go beyond authentication and authorization to govern humans and non-humans as privileged actors, optimally moderating risk in tandem with unused privilege detection, role mining, and continuous IAM event anomaly detection.

Keywords: Identity And Access Management, Privileged Access Management, Zero Trust Architecture, Behavioral Analytics, Regulatory Compliance

1: Risk-Adaptive Privilege Management in Payment and Core Banking Systems

Payment and core banking systems are the most sensitive transactional environments of financial institutions. In these environments, PAM architectures are shifting from rule-based, static models to context-aware, dynamic models, wherein access is granted after assessing risk dynamically, whenever privileged access is initiated by an user [15]. Furthermore, instead of the standing administrative privilege, the system provides a multi-factor risk score of transaction amount thresholds, counterparty reputation indices, temporal behavioral baselines, and geographic access anomalies for just-in-time access provisioning for the given operational task. Zero Trust Architecture (ZTA), as Special Publication 800-207 formalized by the NIST, states that the trust of an access subject is independent of its physical location. ZTA assumes all objects are untrusted until identity authentication and trust evaluation have occurred [1].

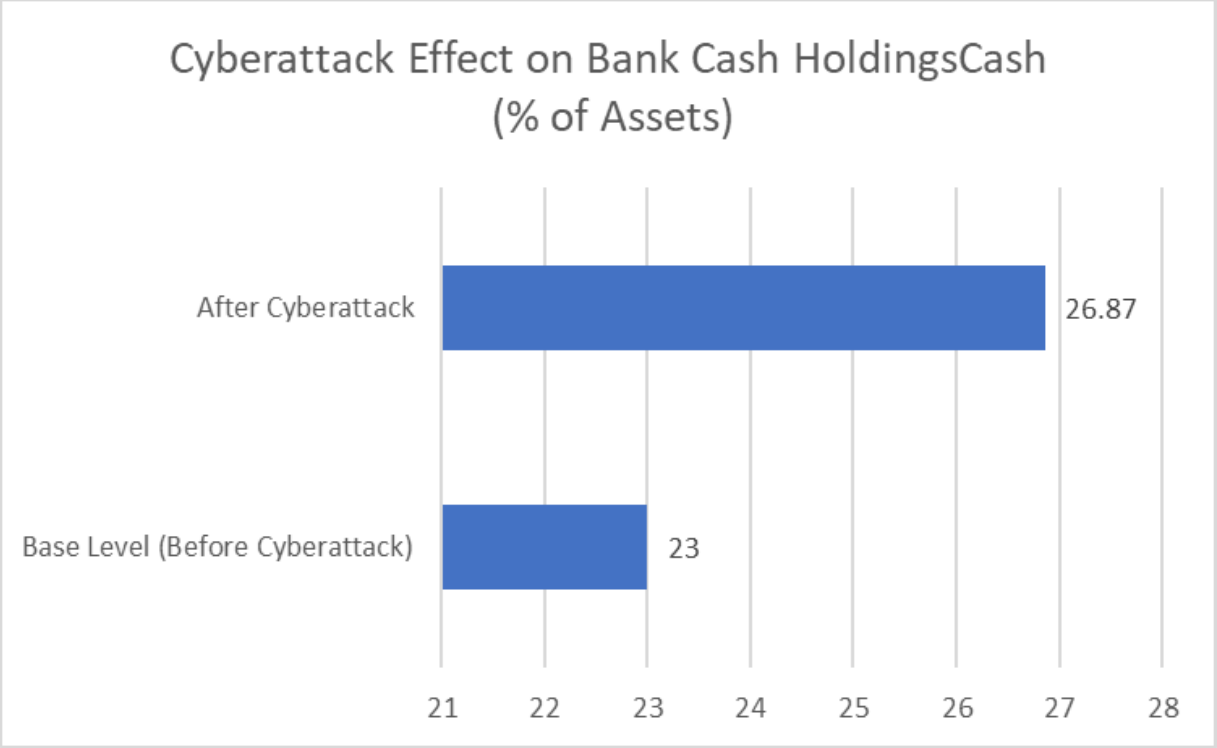
JIT access provisioning is a well-accepted way of governing elevated access in payment systems. In this model, when a database administrator requests access to a payment processing node, he or she is

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

issued a credential to access the node for a limited amount of time, which is revoked after the workflow. This session-based privilege model reduces the time that the organization spends exposed if a cybercriminal gets their hands on the credentials. For financial institutions, the average increase in cash holdings arises in the wake of a cyberattack, from 23.0% to 26.87% of assets. This is how much operational disruption poor privilege governance can cause [2]. Zero Trust Network Access (ZTNA) architectures supplant legacy virtual private network (VPN) implementations by introducing application-layer access policies that validate user identity, device security posture, and risk context of the environment before making any banking resource reachable [1].

For micro-segmented core banking systems, payment processing nodes are implemented in separate enclaves on the network, with least-privileged network policies enforced via granular Access Control Lists (ACLs) to remove lateral movement options after initial system access. The prototype banking applications show that proposed Zero Trust controls have an average system latency of 2 ms and have a transactional throughput of 3.7 to 4.4 transactions per second with 60 concurrent threads under load. The transactional throughput also increases, when the number of concurrent users increases from 20 to 100 threads. Thus, risk-adaptive access enforcement does not degrade the transactional performance [2].



Graph 1: Cash Holdings Before and After Cyberattack [1, 2]

2: Automated Identity Lifecycle Governance in Retail and Branch Operations

Managing user identities for a global bank's network of branch offices posed several functional and security challenges. Manual provisioning processes for new employees to receive role-based access to systems could take days or weeks, while the organization was exposed to the risk and cost of unnecessary over-provisioning when de-provisioning tasks were deferred. Identity Governance and Administration (IGA) tools seek to address these weaknesses by employing automated bidirectional

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

JML workflows with Human Resources Information Systems (HRIS) and managing physical and logical access provisioning and de-provisioning processes based on a single source of truth for identity [3].

Identity lifecycle management involves the 4 stages of identification, authentication, authorization, and accounting and governs how access rights are created, managed, reviewed, and revoked for the branch workforce [4]. When a branch teller is hired, the IGA solution receives a provisioning notification from the HRIS once a record is created. It automatically maps the employee role code to a pre-configured entitlement profile, creating a corresponding set of access credentials to the building access system, workstation directories, core banking applications, and transaction processing applications, allowing provisioning time to be reduced from one-off, multi-day manual processes to sub-hour automated processes. The same bidirectional HRIS integration supports use cases involving movers, such as when a loan officer is promoted to branch manager, entitlements of the old role are revoked and entitlements of the new role provisioned, preventing both access gaps and over-provisioning [3].

Termination workflows represent the portion of the JML process where security is paramount. An IGA system can automatically revoke access across all integrated systems when an employee is terminated, reducing the orphan accounts risk of manual JML workflows. Based on research, there are 3 main identity lifecycle management models: isolated, centralized and federated. The centralized and federated models are more appropriate for branch networks that have large-scale distributed user environments [4]. Role-Based Access Control (RBAC) eases audit trails over time for the changing state of access entitlements, and promotes the principle of least privilege by ensuring that branch staff are allocated the minimum entitlement for their assigned job roles [3].

Workflow Type	Trigger Event	Action Performed
Joiner	New employee hired	Provisions role-based entitlements
Mover	Employee changes role	Revokes old and provisions new entitlements
Leaver	Employee terminated	Revokes access across all integrated systems

Table 1: IGA Workflow Components and Functions [3]

3: Automated Regulatory Compliance and Segregation of Duties Enforcement

Financial services firms are subject to regulatory obligations to log who has access to financial systems, including the Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leach-Bliley Act (GLBA) and the examination standards of the Federal Financial Institutions Examination Council (FFIEC). Compliance with these overlapping requirements, using spreadsheet-based access reviews and ad hoc collation of audit evidence, has become inefficient because of increased technology capabilities and more complex environments. IAM governance platforms solve this problem by continuously enforcing SoD policies in a preventive way, automatically generating tamper-clear audit documentation [5].

SoD enforcement can be implemented by policy engines which look for conflicts in an access provisioning request against a conflict matrix that outlines the role combinations which are incompatible. For example, giving an user payment initiation authority and payment approval authority allows them to self-authorize payments. For example, allowing the same person to post

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

transactions in a general ledger and reconcile them would enable collusion to hide the transactions through manipulation of the reconciliation documents. The policy engine would deny conflicting entitlement provisioning, and typically a workflow to make an exception to the policy would be initiated, which would require business justification and a compensating control to be approved. This model avoids SoD violations by preventing them from occurring in the first place, rather than discovering them through an audit later [5].

Automated access certification campaigns extend entitlement reviews to business process owners and application managers on a predefined schedule aligned with compliance auditing activities. For instance, the PCI DSS suggests quarterly access reviews for systems efficiently storing or processing cardholder data, while SOX-based frameworks could suggest annual reviews of access to financial reporting systems. In IAM systems, certification workitem queues present users with visualizations of their direct reports' current entitlements, highlighting outliers in peer groups such as inconsistent role combinations, or those entitlements no longer used based on activity logging. Centralized compliance reporting repositories aggregate certification, SoD exception and access change audit trails, producing evidence packages for auditors for FFIEC and GLBA compliance purposes without the need for any manual preparation [6].

Conflicting Entitlement Combination	Risk Introduced	Prevention Mechanism
Payment initiation + Payment approval	Fraudulent self-authorization	Policy engine denial
General ledger posting and reconciliation	Concealment of fraudulent entries	Conflict matrix enforcement
Access provisioning + Access certification	Unauthorized entitlement self-approval	SoD exception workflow

Table 2: Segregation of Duties Conflict Examples and Risks [5]

4: Customer Identity and Access Management for Digital Banking Platforms .

CIAM can target retail and commercial banking customers as they access banking services via mobile apps, web portals, or API-connected third-party financial apps. Customer IAM faces extra challenges compared with employee-facing IAM solutions, needing to meet high levels of Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements while also delivering authentication experiences that are as frictionless as possible so as not to drive customers away, and driving high engagement with its digital channels [8].

Modern CIAM uses risk-based adaptive or layered authentication that matches the risk level of the session. Behavioral biometrics engines analyze typing cadence, touch pressure, orientation, and navigation patterns to ensure user identity for the rest of the authenticated session. Perceptual hashing algorithms can be used for biometric processing, generating small 64-bit to 128-bit hashes that can be used as templates without sacrificing accuracy [7]. Device fingerprinting allows known endpoints to be authenticated with little friction but imposes additional authentication challenges on unknown devices. Liveness detection algorithms allow distinguishing biometric captures from attempts to spoof them, as asymmetric cryptographic algorithms are computationally expensive compared to symmetric ones (by as much as 95 times), making hash-based authentication more suitable for resource-limited scenarios [7].

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

With SSO (Single Sign-On), customers have to perform authentication only once rather than on various occasions for multiple banking applications: this decreases the burden of different passwords for users. The average web user maintains around 25 logins with different credentials [8] and inputs passwords into more than 8 websites/web applications daily. In portals, ABAC systems can personalize content based on account attributes, service tiers, and regulatory class. They also enable KYC workflows and continuous identity verification. Improved due diligence can be applied to transaction patterns that indicate a higher risk for These risk factors are common and seen as urgent, as identity theft is responsible for 90% of all data breaches in the United States [8]. New wave digital banks, therefore, require continuously adaptive CIAM architectures.

5: Privileged Access Management in High-Stakes Trading Environments

PAM solutions are particularly challenging in the trading of financial instruments, where there are at least two conflicting requirements. Fast privilege escalation is needed to accommodate the time-sensitive nature of financial trading, while thorough auditing and analysis of insider threat exposure are demanded by financial regulators. Agentless PAM architectures have become a leading choice for mission-critical trading situations due to their lack of operational risk associated with needing agents to be installed on financial trading endpoints, where sub-second outages can expose the enterprise to material financial loss [10].

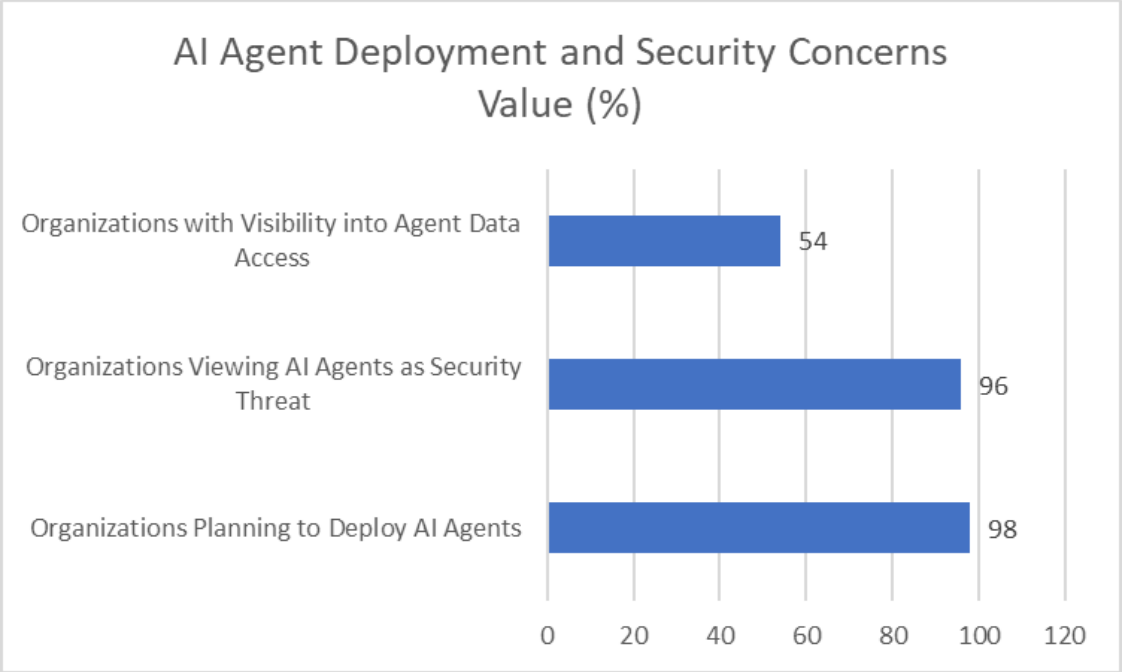
The session brokering technologies broker all privileged sessions through a proxy architecture and record all user sessions (including interaction with applications, commands typed, data extracted, and transactions executed) on a dedicated and secure recording server. No software is installed on secured endpoints. The recorded evidence provides a forensic audit trail that can be used in post-incident investigations, compliance efforts, and dispute resolution. The 2014 JPMorgan Chase data breach, which exposed the highly sensitive personal information of 76 million households and 7 million small businesses, and the 2016 Bangladesh Bank data breach, where the attackers electronically circumvented the bank's network security to transfer $81 million through the SWIFT payment system, are two examples in the financial services sector that support this need for privileged access governance [10].

User and Entity Behavior Analytics (UEBA) algorithms continuously monitor privileged session user activities against the baseline of their typical behavior and peers in a role-based peer group. Behavioral features include time-of-day and day-of-week access distributions, transaction size distributions, data export distributions, and data cross-system navigation. As of 2022, cyberattacks against financial firms rose 80% year-on-year, and algorithmic trading now accounts for more than 60% of US equity trading.

PAM frameworks must also consider non-human privileged actors. With the proliferation of agentic AI systems in trading ecosystems, industry surveys indicate that 98% of organizations plan to deploy AI agents; however, 96% believe that AI agents are an increasing security threat and just 54% have access to visibility into data access behavior of agents [9]. JIT privilege elevation allows users or agents with role authorization to be granted temporary permissions for a specified time, starting and ending based on market activity or tasks being performed, reverting thereafter.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article



Graph 2: AI Agent Adoption vs. Security Concerns [9, 10]

6: AI and Behavioral Analytics for IAM Optimization

IAM Platforms with embedded Artificial Intelligence and Machine Learning capabilities allow us to improve this and evolve from a reactive access control approach to a proactive risk optimization approach. Customary IAM implementations were characterized by heavy manual role definitions and rigid rule-based policy enforcement, which could not cope with the new access patterns of the banking world. This has resulted in the worldwide IAM market reaching USD 15.93 billion in 2022, indicating a growing need to govern access in a smarter and more agile manner within organizations [11;13].

Functioning based on historical access logs, role assignments, and entitlement usage, machine learning can help IAM platforms identify optimization and emerging risk scenarios that rule-based controls cannot identify. Unused privilege detection algorithms identify entitlements that are not being exercised in the environment based on system activity logs over a configurable observation window. Machine learning algorithms are capable of identifying unused privileges and distinguishing them from legitimately infrequently used privileges that are required for business. This allows the attack surface to be automatically reduced by removing unnecessary access using machine learning-based optimization techniques without the need to examine individual user profiles across enterprise populations [11].

To mine roles, many role mining algorithms often apply a clustering algorithm to the user's access patterns to identify clusters of co-occurring entitlements that often appear together. Such AI techniques for biometric authentication have been shown to have a very high accuracy, with deep learning serial fusion obtaining an area under the curve (AUC) value of 0.9996 on 120 works across multiple biometric modalities [11]. However, data-driven approaches are often based on observed access patterns rather than derived from analyzing job function requirements.

The business case for trading environments is even stronger. Research into actual insider threat events at a sample of 3000 VAX sites found the average insider attack to cost the organization $2.7 million, compared to $56000 for a breach by an external hacker (see [12]). Behavioral analytics engines continuously operate on streams of IAM events and look for anomalies such as impossible travel, unusual data transfers, abnormal privileged access, and access across unrelated systems.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

When these indicators are found, they can alert security operations teams to investigate credential compromise or insider threat activity before large-scale security breaches occur. Spot-checking of these and other indicators in real-time can, if done early, ease targeted responses [12] .

Conclusion

Managing digital identities and access control within a complex, multi-tiered financial ecosystem demands a unified, intelligence-driven architecture for achieving business agility, regulatory compliance, and dynamic threat hardening. Risk-adaptive privilege management solutions based on the Zero Trust model contribute to the removal of static standing conditions that adversaries seek to exploit. Furthermore, Just-in-Time provisioning enables the short-lived availability of elevated privileges for the duration of specific operational activities [14]. Automated identity lifecycle governance eliminates the latency and errors of manual provisioning. It continuously aligns entitlements with actual role needs throughout the employee lifecycle, entirely revoking access at termination, and proactively checks for conflicting access combinations before they can manifest as either audit or fraud opportunities through Preventive Segregation of Duties enforcement. Automated audits via certification campaigns also continuously generate compliance evidence by tracing to overlapping regulations. In customer-centered authentication models, behavioral biometrics and risk-adjusted challenge/authentication, adaptive to the assessed context of the session, are deployed to balance user experience friction against the high threshold of identity assurance that KYC and AML bring to the model. With the expanding privileged access surface, session recording, behavioral analytics, and agentic AI governance frameworks are emerging in trading and trading-like environments, in which real-time algorithmic oversight is exercised over humans and machines. This evolution from an IAM vigilante to a proactive risk-optimizing platform stems from the AI capabilities built into IAM platforms. Machine learning helps optimize role hierarchies, detect unused entitlements, and monitor anomalous account actions to identify potential credential compromise or insider threat activity before it becomes a security incident. Whether measured in the monetary impact of breach remediation, lack of compliance with regulations, or damage to reputation, the financial case for strong access governance and an enterprise IAM architecture is inescapable.

References

[1] Yuanhang He, et al., "A survey on zero trust architecture: Challenges and future trends," Wireless Communications and Mobile Computing, 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1155/2022/6476274
[2] Clement Daah et al., "Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework," MDPI, 2024. [Online]. Available: https://doi.org/10.3390/electronics13050865
[3] Nikhil Ghadg, "Optimizing identity management: Key strategies for effective governance and administration," International Journal of Security, Privacy and Trust Management (IJSPTM), 2024. [Online]. Available: https://www.researchgate.net/profile/Nikhil-Ghadge-2/publication/382741790
[4] Jenny Torres et al., "A survey on identity management for the future network," IEEE, 2012. [Online]. Available: https://www.researchgate.net/profile/Michele-Nogueira/publication/260671142
[5] Kevin W. Kobelsky, "A conceptual model for segregation of duties: Integrating theory and practice for manual and IT-supported processes," International Journal of Accounting Information Systems, 2014. [Online]. Available: https://www.academia.edu/112631321/A_conceptual_model_for_segregation_of_duties_Integrating_theory_and_practice_for_manual_and_IT_supported_processes
[6] Jing Liu et al., "A Survey of Payment Card Industry Data Security Standard," IEEE Communications Surveys & Tutorials, 2010. [Online]. Available:

https://www.academia.edu/90091285/A_Survey_of_Payment_Card_Industry_Data_Security_Standard

[7] Parwinder Kaur Dhillon, Sheetal Kalra (2017). "A lightweight biometrics-based remote user authentication scheme for IoT services": Journal of Information Security and Applications, https://www.academia.edu/84873006/A_lightweight_biometrics_based_remote_user_authentication_scheme_for_IoT_services

[8] Ishaq Azhar Mohammed, Systematic Review Of Identity Access Management In Information Security. IJIERT, 2017. https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887659

[9] Shaina Raza, "TRiSM for Agentic AI: A Review of Trust, Risk, and Security Management in LLM-based Agentic Multi-Agent Systems," arXiv, 2025. https://arxiv.org/pdf/2506.04133

[10] Kenneth Chukwujekwu Nwafor, "Leveraging data mining and cybersecurity techniques to enhance algorithmic trading performance and forensic investigations in financial markets," International Journal of Science and Research Archive, (2024). https://www.researchgate.net/profile/Kenneth-Nwafor-3/publication/387511052

[11] Jesús Vegas and César Llamas, "Opportunities and Challenges of Artificial Intelligence Applied to Identity and Access Management in Industrial Environments," MDPI, (2024). https://www.mdpi.com/1999-5903/16/12/469

[12] Eric Shaw et al., "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider," cerias. Purdue (1998). https://homes.cerias.purdue.edu/~mkr/sab.pdf

[13] Beeyani, G. Optimizing Kitchen Operations Through Process Innovation And Smart Technologies In The Hospitality Sector. *Lex Localis*, *22*(S4), (2024): 391-401

[14] Paula Alejandra Diaz Munoz Resilient Urban Design Evaluating Mixed-Use Development Models In Emerging Economies. *IPHO-Journal of Advance Research in Business Management and Accounting*. 2, 12 (Dec. 2024), 31–39. DOI:https://doi.org/10.5281/zenodo.19354359.

[15] Quintero, F. A. " Reducing Production Time without Compromising Quality: Optimization Strategies in High-End VFX Simulations." *Sarcouncil Journal of Engineering and Computer Sciences,* 3.8 (2024): pp 1-8.