International Journal of Multidisciplinary Research and Growth Evaluation.

Risk-Based Approach to Corporate Investigations and Insider Threat Mitigation in Multinational Organizations

Ayomipo Ewuola
Nigeria LNG Ltd., Nigeria

* Corresponding Author: **Ayomipo Ewuola**

Article Info

ISSN (online): 2582-7138
Volume: 04
Issue: 02
March-April 2023
Received: 15-03-2023
Accepted: 19-04-2023
Page No: 811-821

Abstract
Insider threats represent a significant and evolving risk to multinational organizations, challenging traditional security and investigative paradigms due to the complexity of diverse legal, cultural, and operational environments. This explores a risk-based approach to corporate investigations and insider threat mitigation, grounded in extensive investigative leadership experience across multiple regions. The risk-based methodology emphasizes the identification, prioritization, and management of insider threats by aligning investigative efforts with the organization's strategic risk appetite and operational context. The study examines the multifaceted nature of insider threats including malicious, negligent, and inadvertent actions and highlights regional variations in threat motivations and manifestations. It discusses the necessity of integrating risk assessment frameworks tailored to differing geopolitical and regulatory landscapes, enabling organizations to effectively prioritize investigative resources and tailor mitigation strategies. This further outlines a strategic investigative methodology that balances rigorous data-driven analysis with cultural and legal sensitivities inherent in global operations. The use of advanced forensic tools, behavioral analytics, and real-time monitoring systems is emphasized as critical enablers for proactive threat detection and response. Additionally, the role of leadership in fostering a security-conscious culture, encouraging cross-regional collaboration, and ensuring transparent communication is explored as a key success factor. Challenges such as jurisdictional constraints, resource disparities, and information sharing complexities are addressed, alongside practical recommendations for enhancing organizational resilience through adaptive policies and continuous capacity building. The study concludes by advocating for a dynamic, integrated approach that leverages technology, leadership, and localized understanding to mitigate insider risks effectively. This contributes valuable insights into the evolving domain of corporate investigations, proposing a comprehensive framework for multinational organizations seeking to strengthen their insider threat defenses through a risk-based lens.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.2.811-821

Keywords: Risk-based, Approach, Corporate investigations, Insider threat, Mitigation, Multinational organizations

1. Introduction

In today's increasingly interconnected global economy, multinational organizations face an evolving and complex array of security challenges, among which insider threats stand out as particularly insidious and damaging (Akpe *et al*., 2020; EYEREGBA *et al*., 2020). Insider threats ranging from malicious sabotage and data theft to inadvertent policy breaches pose significant risks to the confidentiality, integrity, and availability of critical organizational assets (Mgbame *et al*., 2020; Ofori-Asenso *et al*., 2020). The complexity of these threats is compounded in multinational corporations (MNCs) by diverse operational environments, varying regulatory frameworks, and cultural differences that influence employee behavior and

organizational norms (EYEREGBA *et al*., 2020; Kisina *et al*., 2021). Consequently, traditional investigative models that rely on uniform procedures and reactive responses are no longer sufficient to address the dynamic nature of insider threats in these complex settings (Omisola *et al*., 2020; ONIFADE *et al*., 2020).

The importance of adopting a risk-based investigative approach cannot be overstated in this context. Such an approach enables organizations to prioritize resources, focus on the most critical vulnerabilities, and tailor investigative methodologies to the unique risk profiles of their global operations (Akinsooto *et al*., 2014; Iyabode, 2015). By integrating risk assessment directly into the investigative process, organizations can move beyond reactive investigations toward proactive risk mitigation and strategic insider threat management (EZEANOCHIE *et al*., 2021; Abayomi *et al*., 2021). This approach enhances the effectiveness of investigations by aligning them with organizational objectives and risk appetite, ensuring that responses are timely, efficient, and legally compliant across jurisdictions (Abayomi *et al*., 2021; Abisoye and Akerele, 2021).

The purpose of this review is to explore and articulate a conceptual framework for applying a risk-based approach to corporate investigations and insider threat mitigation within multinational organizations. Drawing from investigative leadership experience across diverse regions, this seeks to provide a comprehensive understanding of the challenges and opportunities inherent in managing insider risks on a global scale. The objectives include examining the nature and drivers of insider threats in multinational contexts, outlining the components of an effective risk-based investigative strategy, and highlighting practical considerations for implementation across varied cultural and regulatory landscapes.

Multinational operations inherently present significant challenges to insider threat management (Afolabi and Akinsooto, 2021; Kisina *et al*., 2021). Variations in labor laws, privacy regulations, and investigative authority necessitate careful navigation to maintain legal and ethical compliance while conducting thorough investigations. Moreover, cultural diversity plays a crucial role in shaping employee attitudes toward security, reporting, and cooperation with investigations. For instance, norms regarding privacy, loyalty, and whistleblowing differ widely between regions, affecting the detection and handling of insider threats. Additionally, operational differences such as varying levels of technological maturity and resource availability across subsidiaries complicate the establishment of standardized investigative protocols. These complexities require a flexible yet structured investigative framework capable of adapting to local conditions while maintaining a cohesive global strategy.

The rising complexity of insider threats in multinational corporations demands a sophisticated, risk-based approach to investigations and mitigation. This aims to address the operational and cultural challenges faced by global organizations and propose a conceptual framework that integrates risk assessment, cross-jurisdictional coordination, and adaptive investigative techniques. By doing so, it contributes to the ongoing discourse on enhancing corporate security resilience in the face of increasingly sophisticated insider risks in multinational environments.

2. Methodology

For this conceptual paper on a risk-based approach to corporate investigations and insider threat mitigation in multinational organizations, a systematic literature review was conducted following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure comprehensive and transparent research synthesis. Initial database searches were performed across multiple academic and industry sources, including Scopus, Web of Science, IEEE Xplore, and Google Scholar, covering publications from 2010 to 2025. Search terms combined keywords and phrases such as "insider threat," "corporate investigations," "risk-based approach," "multinational organizations," "investigative leadership," and "insider threat mitigation."

The identification phase yielded 482 records. After removing duplicates, 430 unique articles remained for screening. Titles and abstracts were reviewed against inclusion criteria emphasizing studies and reports related to corporate investigations, insider threat management strategies, risk assessment methodologies, and cross-cultural or multinational contexts. Exclusion criteria eliminated articles unrelated to corporate investigations, non-English publications, and papers focusing solely on technical cybersecurity solutions without organizational or investigative dimensions.

A total of 72 articles progressed to full-text review, during which detailed evaluation assessed relevance, methodological rigor, and applicability to multinational operational challenges. Studies addressing regulatory compliance, cultural diversity, risk prioritization, and investigative frameworks were prioritized. This process resulted in 35 key sources incorporated into the conceptual synthesis.

Data extraction focused on thematic elements such as risk assessment models, investigative leadership practices, insider threat typologies, and multinational organizational dynamics. The qualitative synthesis integrated findings with the author's extensive investigative leadership experience across regions, enabling development of a nuanced conceptual framework.

The PRISMA flowchart and checklist were used to document the review stages, ensuring transparency and reproducibility. This rigorous methodological approach supports the validity of the conceptual framework proposed and provides a robust foundation for future empirical research in the field of insider threat mitigation in complex multinational settings.

2.1 Conceptual Foundations

Corporate investigations and insider threats are critical concerns for multinational organizations operating in increasingly complex and dynamic environments. Corporate investigations refer to systematic, methodical inquiries conducted within an organization to detect, analyze, and resolve incidents involving fraud, misconduct, regulatory violations, or security breaches (Mgbame *et al*., 2021; Ogbuefi *et al*., 2021). These investigations often require multidisciplinary approaches, blending forensic accounting, legal analysis, cybersecurity, and human resources to uncover facts and mitigate risks. Insider threats, on the other hand, pertain to risks posed by individuals within the organization such as employees, contractors, or partners who have authorized access but may intentionally or unintentionally cause harm through data theft, sabotage, espionage, or policy violations.

A risk-based approach to corporate investigations and insider threat mitigation is grounded in the principle of prioritizing resources and efforts according to the likelihood and potential impact of threats. Unlike reactive or purely compliance-driven models, this approach emphasizes proactive identification, continuous assessment, and tailored responses aligned with organizational risk appetite. The core principles of risk-based methodologies include systematic risk assessment, integration of intelligence from multiple sources, prioritization based on threat severity, and dynamic adaptation to evolving risk landscapes (Ogeawuchi *et al*., 2021; Ogundipe *et al*., 2021). By focusing investigative resources on high-risk areas, organizations can enhance efficiency, reduce operational costs, and improve the overall effectiveness of security measures.

Key components of insider threat frameworks within a risk-based model typically encompass risk identification, monitoring, prevention, detection, investigation, and remediation. Risk identification involves understanding potential insider threat vectors by analyzing organizational vulnerabilities such as access controls, employee behavior patterns, and critical asset exposure. Monitoring utilizes technological solutions like user behavior analytics (UBA), access logs, and anomaly detection systems to flag suspicious activities. Prevention includes policies, training, and cultural initiatives aimed at reducing insider risks. Detection and investigation involve detailed examination of alerts and incidents, combining data analysis with human judgment to distinguish between false positives and genuine threats (Onifade *et al*., 2021; Ajayi and Akanji, 2021). Finally, remediation focuses on mitigating damage and implementing corrective measures to prevent recurrence.

Leadership plays a pivotal role in shaping the effectiveness of investigative processes, especially within multinational organizations where cultural diversity, jurisdictional complexity, and operational scale add layers of challenge. Investigative leadership entails setting strategic direction, ensuring resource allocation, fostering cross-functional collaboration, and maintaining adherence to legal and ethical standards. Leaders must balance global consistency with local contextual sensitivity, adapting investigative protocols to regional regulatory frameworks and cultural norms without compromising overall risk management objectives (Akinsooto, 2013; Abisoye and Akerele, 2022). Moreover, strong leadership drives the establishment of a risk-aware organizational culture, where employees at all levels recognize the importance of security and compliance, thereby reducing insider threat opportunities.

In multinational settings, leadership must also navigate complexities such as varying legal requirements, differing attitudes toward privacy and whistleblowing, and disparate technological infrastructures. Effective leaders leverage regional expertise and foster communication channels between headquarters and local entities to ensure timely and coordinated investigations. They champion the integration of investigative teams, legal counsel, cybersecurity units, and human resources, creating unified responses to insider threats. Additionally, leadership commitment to ongoing training, technological innovation, and policy refinement reinforces the organization's resilience against insider risks (EYEREGBA *et al*., 2021; Akinsooto *et al*., 2021).

Corporate investigations and insider threat mitigation are intertwined elements critical to safeguarding multinational organizations. A risk-based approach provides a structured, proactive framework that enhances the strategic allocation of investigative resources and improves threat detection and response. Insider threat frameworks grounded in risk principles encompass comprehensive components from identification through remediation, supported by advanced technologies and organizational policies. Central to successful implementation is effective leadership, which navigates cultural and regional complexities to ensure cohesive, compliant, and adaptive investigative practices across global operations (Akpe *et al*., 2022; Attah *et al*., 2022). This conceptual foundation sets the stage for developing more refined, context-sensitive strategies that address the unique challenges of insider threat mitigation in multinational environments.

2.2 Insider Threat Landscape in Multinational Organizations

The insider threat landscape in multinational organizations is increasingly complex and multifaceted, influenced by a range of operational, legal, cultural, and technological factors as shown in figure 1. As organizations expand their global footprint, they become more susceptible to insider risks that differ across regions in both form and intensity. These threats emanate from individuals within the organization employees, contractors, or partners who exploit their authorized access either maliciously or inadvertently, posing significant risks to data integrity, corporate reputation, and operational continuity (EZEANOCHIE *et al*., 2022; Hlanga, 2022).

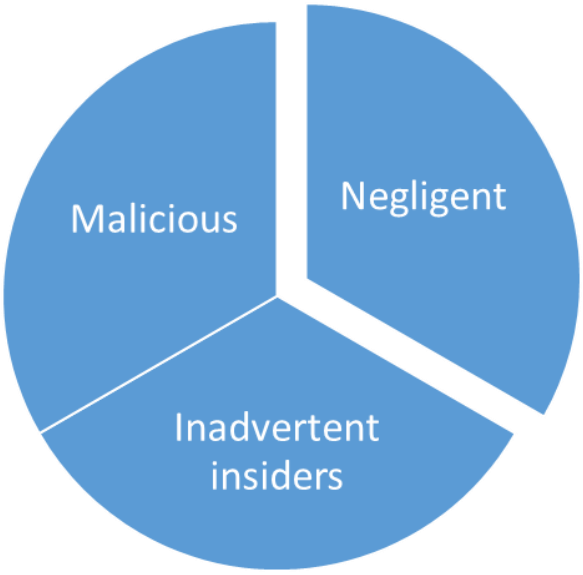

Fig 1: Types of insider threats

Insider threats are generally categorized into three main types: malicious, negligent, and inadvertent insiders. Malicious insiders act with deliberate intent to cause harm, motivated by financial gain, ideological beliefs, revenge, or coercion. These actors are often the most damaging, using their intimate knowledge of systems and processes to evade detection. Negligent insiders, by contrast, are not driven by ill intent but demonstrate carelessness in handling sensitive data, failing to follow established security protocols or engaging in risky behaviors such as using unsecured devices. Inadvertent insiders include individuals who unwittingly fall victim to social engineering, phishing, or other manipulation tactics that result in unauthorized data access or disclosure

(Johnson *et al*., 2022; Kisina *et al*., 2022).

Regional variations further complicate insider threat management. In regions with high levels of political instability or economic uncertainty, motivations for malicious insider activity may be more prevalent due to increased vulnerability to bribery or coercion. In developed regions, negligent and inadvertent threats may dominate due to high levels of system access and digitization. In contrast, in parts of Asia and Africa, insider threats may stem more from socio-economic pressures and limited employee vetting procedures, particularly in outsourced or third-party contractor environments.

Navigating the legal, cultural, and regulatory environments across jurisdictions presents significant challenges. Privacy laws in the European Union, such as the General Data Protection Regulation (GDPR), impose strict limitations on employee monitoring, complicating proactive detection of insider threats. Conversely, in countries with less stringent privacy protections, aggressive monitoring may be legally permissible but culturally stigmatized, affecting employee morale and trust (Kisina *et al*., 2022; Adaobi *et al*., 2022). Cultural attitudes toward whistleblowing also vary significantly what may be encouraged and legally protected in the U.S. might be viewed as disloyal or even dangerous in countries with weak labor protections or authoritarian governance structures.

Several case examples illustrate the intricacies of insider threat mitigation across different geographies. In 2018, a disgruntled IT administrator at an Australian energy company deliberately deleted critical data after being terminated, exploiting retained access credentials a classic example of a malicious insider exploiting delayed access revocation. In another case from India, employees at a global financial services firm inadvertently exposed sensitive client data due to poor cybersecurity hygiene and inadequate awareness training an illustration of negligent behavior compounded by organizational oversight. Meanwhile, in Germany, a multinational manufacturing company faced regulatory hurdles in investigating a suspected insider leak due to strict data privacy laws that limited access to employee email records. These examples underscore the importance of adopting nuanced, context-aware investigative strategies tailored to local conditions while maintaining a unified global risk posture (Ogundipe *et al*., 2022; Onifade *et al*., 2022).

The insider threat landscape in multinational corporations is shaped by diverse actors and regional dynamics. Effective mitigation requires an understanding of different types of insider threats, adaptation to regional threat profiles, and navigation of complex legal and cultural environments. Organizations must invest in context-sensitive threat intelligence, establish harmonized yet flexible policies, and foster cross-cultural awareness to address the evolving risk posed by insiders. By aligning global strategy with local realities, multinational organizations can strengthen their resilience against internal threats and safeguard their most critical assets (Vindrola-Padros and Johnson, 2022; Abisoye and Akerele, 2022).

2.3 Risk Assessment and Prioritization

Effective insider threat mitigation in multinational organizations hinges on the robustness of risk assessment and prioritization processes. These processes enable organizations to allocate resources efficiently, develop context-sensitive intervention strategies, and align with corporate governance and compliance obligations as shown in figure 2. A structured approach to identifying and categorizing risks based on both likelihood and impact forms the foundation for a proactive and adaptive risk management framework (Abisoye *et al*., 2022; Abisoye, 2023).

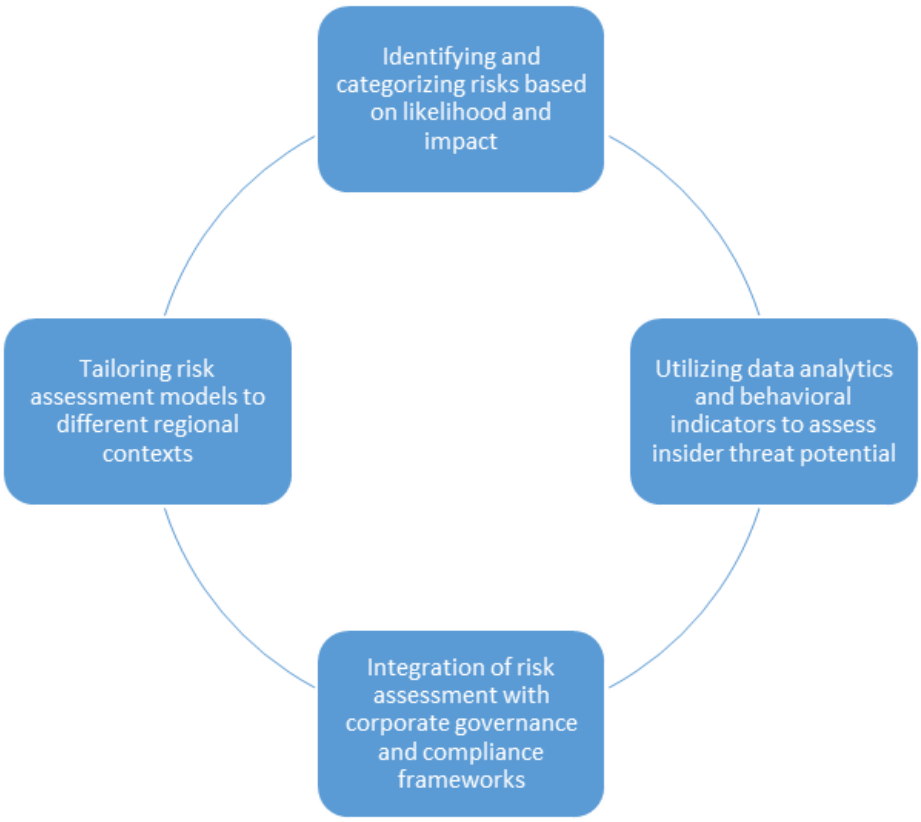

Fig 2: Risk Assessment and Prioritization

The first critical step in any risk-based investigative model is identifying and categorizing risks. This involves mapping potential insider threat vectors ranging from unauthorized data access and intellectual property theft to sabotage and reputational damage. Risks are categorized based on two primary dimensions: the likelihood of occurrence and the severity of their impact. High-likelihood, high-impact risks such as access misuse by privileged users or collusion with external actors require top-priority mitigation. Conversely, low-likelihood, low-impact risks may warrant periodic monitoring but not immediate action. This prioritization model ensures that investigative efforts and preventive measures focus on the most consequential threats.

To enhance the accuracy and depth of assessments, data analytics and behavioral indicators are increasingly employed. Sophisticated systems now analyze vast datasets, including access logs, user activity monitoring, and communication patterns, to detect anomalies suggestive of insider risk. Behavioral analytics tools, powered by machine learning algorithms, can identify subtle deviations from baseline behavior, such as sudden changes in file access frequency, unusual login times, or atypical communication networks (Akpe *et al*., 2023; Abisoye, 2023). These indicators, when contextualized, help preemptively identify potential insider threats and provide actionable intelligence for investigators.

However, applying a standardized model across all regions may lead to blind spots due to variations in organizational culture, regulatory constraints, and threat typologies. Thus, tailoring risk assessment models to different regional contexts is essential. In jurisdictions with strong labor protections and privacy regulations (e.g., the EU), insider threat detection must be designed to comply with legal standards while respecting cultural expectations around privacy. In contrast, in regions with high economic disparity or political instability, risk assessments may prioritize social and financial stress indicators that increase susceptibility to insider collusion or coercion (Esan *et al*., 2023; Kalu *et al*., 2023). Tailoring models also includes incorporating local threat intelligence, understanding regional business practices, and adapting investigative protocols accordingly.

Another critical success factor is the integration of risk assessment with corporate governance and compliance frameworks. Embedding insider threat assessments within broader enterprise risk management (ERM) systems allows for a unified view of operational vulnerabilities and ensures alignment with organizational policies. Furthermore, integration with compliance functions ensures that threat mitigation efforts adhere to internal controls, external regulatory requirements, and audit standards. For instance, aligning risk assessment processes with the ISO 31000 risk management standard or the COSO ERM framework enhances the transparency and accountability of insider threat programs. Regular reporting to compliance committees and board-level risk subcommittees ensures oversight and elevates the strategic importance of insider threat mitigation (Kisina *et al*., 2023; Ochuba *et al*., 2023).

Additionally, incorporating risk-based assessments into the corporate governance fabric fosters a culture of risk awareness across all levels of the organization. Business units become more attuned to recognizing early signs of insider threats, and leadership is better equipped to make informed decisions regarding risk tolerance, investment in mitigation tools, and escalation protocols. Such an integrated and prioritized approach improves the organization's resilience against internal threats and aligns operational security with strategic objectives.

The effectiveness of insider threat mitigation in multinational organizations is significantly enhanced by a systematic and dynamic risk assessment process. Categorizing risks by likelihood and impact, leveraging behavioral analytics, adapting models to regional contexts, and integrating assessments into corporate governance structures provide a comprehensive framework for threat prioritization. As threat landscapes evolve, continuous refinement of these processes will be essential for safeguarding critical assets and maintaining operational integrity (Onifade *et al*., 2023; Afolabi and Akinsooto, 2023).

2.4 Insider Threat Mitigation Measures

Insider threats pose a persistent and multifaceted risk to multinational organizations, often exploiting trusted access to compromise data, disrupt operations, or undermine organizational integrity (Saxena *et al*., 2020; Zhang, 2020). As insider threats may originate from malicious intent, negligence, or inadvertent actions, a comprehensive mitigation strategy must incorporate preventive controls, robust detection mechanisms, effective response protocols, and leadership-driven cultural transformation as shown in figure 3. These components work in concert to reduce vulnerabilities, enhance resilience, and uphold corporate accountability.

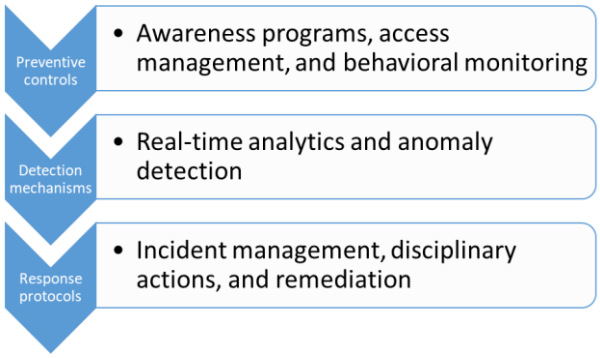

Fig 3: Insider Threat Mitigation Measures

Preventive controls are the first line of defense against insider threats. Among these, awareness programs are essential to educate employees on policies, ethical standards, data sensitivity, and reporting mechanisms. Effective awareness campaigns are continuous, culturally sensitive, and supported by training modules tailored to specific job roles and risk exposures. These programs promote vigilance and discourage risky behavior through regular communication and reinforcement of consequences.

Additionally, access management plays a pivotal role in limiting the exposure of sensitive assets. Role-based access control (RBAC), least privilege principles, and dynamic access review processes ensure that employees have access only to the information and systems required for their functions (Uddin *et al*., 2019; Nyame and Qin, 2020). Integration of physical and digital access controls—such as biometric authentication or multi-factor login protocols—further enhances access security.

Behavioral monitoring complements these controls by enabling the proactive identification of potentially harmful actions. By establishing baseline behavioral profiles,

organizations can detect deviations that may signal malicious or negligent insider activity.

Detection mechanisms must provide real-time insights into insider activity. Advanced analytics and anomaly detection tools, often powered by artificial intelligence and machine learning, offer organizations the capacity to process vast volumes of data across different environments. These systems identify patterns that traditional rule-based monitoring may overlook, such as subtle shifts in communication tone or digital footprint. For multinational organizations, detection systems must also account for regional behavioral nuances to minimize false positives and increase detection accuracy (Kaul and Khurana, 2021; Festini, S.B. and Katz, 2021).

Once a threat is identified, response protocols guide the containment and resolution process. Incident management frameworks should be well-defined, tested, and scalable to various types of insider threat scenarios. These include immediate containment steps (e.g., revoking access), forensic investigations, and engagement of legal or compliance teams where necessary. Organizations must also have clear disciplinary procedures, ensuring fairness, adherence to labor laws, and respect for employee rights across jurisdictions.

Remediation measures, such as policy updates, retraining, and system reconfiguration, are crucial for preventing recurrence. Multinational operations require localized adaptation of these protocols, considering legal requirements, union contracts, and data protection regulations specific to each region. Incident postmortems and lessons-learned exercises enhance institutional learning and continuous improvement.

Underlying the success of all these measures is the role of leadership in cultivating a security-aware organizational culture. Senior executives and middle managers must model ethical behavior, champion risk-awareness initiatives, and allocate resources for security programs. Establishing Chief Insider Threat Officers (CITOs) or cross-functional risk committees can ensure alignment across business units and geographies. When leaders prioritize insider risk at the strategic level, it signals to employees the seriousness of the issue and encourages proactive engagement (Bell *et al*., 2019; Lu *et al*., 2019).

Moreover, leadership must balance security enforcement with employee trust. Overly invasive monitoring or disproportionate penalties can damage morale and erode psychological safety. A mature security culture encourages responsible behavior through transparency, feedback mechanisms, and recognition of ethical conduct.

Insider threat mitigation in multinational organizations requires a multi-layered strategy. Preventive controls, detection tools, and response protocols must be integrated and supported by leadership committed to fostering a security-conscious culture (Ali *et al*., 2021; Khando *et al*., 2021). By aligning these efforts with local regulatory contexts and global best practices, organizations can significantly reduce insider threat risks and protect critical assets in a complex and evolving threat landscape.

2.5 Cross-Regional Collaboration and Communication

In multinational organizations, insider threat mitigation efforts cannot be effective without strong cross-regional collaboration and communication. With operations spread across multiple countries each with distinct legal frameworks, cultural values, and security postures establishing a unified approach to managing insider threats poses both opportunities and complexities (Adkins *et al*., 2020; Varga *et al*., 2021). A successful strategy relies on harmonizing global standards with local relevance, enabling secure information sharing, navigating jurisdictional constraints, and fostering trust among diverse teams.

To begin with, establishing global standards with local adaptability is critical. A centralized corporate security policy provides consistency, accountability, and strategic alignment. However, rigid global protocols may not account for the nuances of local laws, labor regulations, and cultural expectations. Therefore, multinational organizations must adopt a framework that delineates universal security principles such as risk-based decision-making, least privilege access, and data protection while allowing regional offices to tailor implementation to their local contexts. This “glocal” model ensures that security measures are both effective and compliant.

Information sharing between regions and with external stakeholders enhances situational awareness and accelerates incident response. Threat intelligence sharing across business units and geographies can identify emerging insider threat trends, reveal cross-border attack patterns, and support predictive risk assessments. Organizations should establish formal communication protocols and secure collaboration platforms to facilitate timely and confidential exchanges of information (Zelenay *et al*., 2019; Babun *et al*., 2021). Moreover, partnerships with government agencies, industry peers, and cybersecurity vendors can bolster defenses by contributing to shared threat databases or participating in Information Sharing and Analysis Centers (ISACs).

However, these benefits must be balanced against managing jurisdictional challenges and data privacy concerns. Different countries have varying degrees of legal acceptance regarding employee surveillance, data transfer, and whistleblower protections. The European Union’s General Data Protection Regulation (GDPR), for instance, places strict limits on employee monitoring and international data flows. Organizations must engage local legal counsel and compliance teams to ensure that threat mitigation practices such as behavioral analytics or forensic investigations do not violate local laws. Secure data localization, encryption, and anonymization techniques can support privacy while enabling cross-border analysis.

Building a sustainable collaboration model also demands trust and transparency within diverse teams. Cross-cultural communication differences, varying risk perceptions, and hierarchical management styles can hinder cooperation and lead to inconsistent practices. Leadership must invest in intercultural competence training and create inclusive forums for dialogue. Encouraging knowledge sharing through joint task forces, rotating security personnel across regions, and hosting global threat scenario exercises fosters mutual understanding and professional rapport (Tang, 2019; Birdi *et al*., 2021). Establishing clear roles, shared responsibilities, and mutual respect ensures that security teams across regions operate as a cohesive unit rather than isolated silos.

Moreover, transparent communication about insider threat policies and investigation procedures enhances employee buy-in. Staff must be informed of their rights, responsibilities, and the rationale behind monitoring activities. Confidential reporting channels, periodic feedback loops, and visible executive sponsorship contribute to a workplace environment where employees feel safe to report concerns without fear of retaliation. This psychological

safety is crucial for the early detection of insider threats and encourages ethical behavior across the organization.

Effective cross-regional collaboration and communication are foundational to a risk-based approach to insider threat mitigation in multinational corporations. By balancing global standards with local implementation, facilitating secure information sharing, addressing legal and privacy concerns, and fostering a culture of trust and transparency, organizations can create a resilient and unified security posture (Sheikh *et al*., 2021; Brass and Sowell, 2021). These efforts not only enhance insider threat detection and response but also strengthen organizational integrity in an increasingly interconnected and complex global business environment.

2.6 Lessons from Investigative Leadership Experience

Investigative leadership in multinational organizations involves navigating a complex terrain shaped by diverse legal frameworks, cultural values, organizational structures, and evolving threat landscapes. Drawing on experiential insights, key lessons emerge regarding success factors, common pitfalls, strategic leadership approaches, and methods to enhance investigative agility (Knight *et al*., 2020; Bergmann *et al*., 2021). These lessons are instrumental for building resilient and effective corporate investigation teams in the face of insider threats and other corporate risks.

Key success factors in multinational investigations include cross-cultural competence, regulatory awareness, and stakeholder engagement. Successful investigations often hinge on a clear understanding of regional legal systems, from data protection laws to labor rights. A thorough pre-investigative risk assessment that maps jurisdictional constraints and cultural nuances ensures lawful and respectful procedures. Equally important is early stakeholder alignment engaging legal counsel, HR, compliance officers, and local security teams fosters trust, access to information, and operational continuity. Another critical factor is the deployment of standardized investigative protocols that are adaptable but consistent, ensuring integrity, evidence admissibility, and transparency across all regions (Stoyanova *et al*., 2020; Khan *et al*., 2021).

Common pitfalls in multinational investigations typically revolve around miscommunication, jurisdictional overreach, and inconsistent application of procedures. One frequent error is assuming that investigative practices effective in one region can be seamlessly applied elsewhere without modification. Another pitfall is neglecting the human dimension insufficient cultural sensitivity can alienate employees or provoke resistance, undermining cooperation. These risks can be mitigated by investing in cultural intelligence training, establishing locally embedded investigative liaisons, and maintaining regular dialogue with regional leadership.

Strategic leadership approaches play a pivotal role in fostering collaboration and resilience during investigations. Investigative leaders must demonstrate ethical clarity, decisiveness, and adaptability. A transformational leadership style one that inspires purpose, encourages transparency, and empowers regional teams proves especially effective. Leaders should emphasize shared values such as integrity, fairness, and confidentiality, which transcend cultural differences and unify global teams. Building diverse investigative task forces with representation from different regions ensures broader perspectives and reinforces a sense of inclusion and shared responsibility. Additionally, scenario-based training programs, ethical dilemma workshops, and real-time simulations help sharpen investigative judgment and promote readiness.

Another strategic necessity is enhancing investigative agility to address evolving threats. Insider threats are becoming increasingly sophisticated, often blending digital footprints with physical actions. Agile investigations require dynamic tools and rapid response capabilities. Integrating real-time data analytics, behavioral monitoring, and forensic technologies into the investigative workflow improves detection and speeds up resolution (Puzis *et al*., 2020; Holt *et al*., 2021). Moreover, agile methodologies such as iterative evidence reviews and cross-functional sprint teams allow organizations to adjust course swiftly as new information emerges. Embedding agility also involves cultivating a culture of continuous improvement, where lessons learned from each investigation inform future protocols and training. Furthermore, leadership must institutionalize post-incident learning and accountability. Structured debriefs that involve all key stakeholders can identify process inefficiencies, training gaps, and systems vulnerabilities. These sessions should be non-punitive and focused on constructive outcomes, reinforcing a culture of openness and continuous learning. Metrics such as time-to-resolution, stakeholder satisfaction, and policy compliance should guide performance evaluation and resource allocation.

The experience of investigative leadership in multinational organizations highlights the importance of cultural fluency, regulatory alignment, stakeholder engagement, and ethical consistency. Avoiding common pitfalls through adaptive procedures, clear communication, and inclusive strategies strengthens investigative integrity (Bernstein *et al*., 2020; Khatibi *et al*., 2021). Strategic leadership that embraces collaboration and agility is essential to address complex and evolving threats. As insider risks become more intricate and geographically dispersed, the ability to lead investigations with precision, empathy, and resilience will define the effectiveness of global corporate security functions.

2.7 Future Trends and Recommendations

As multinational corporations (MNCs) navigate a rapidly evolving threat landscape, the future of corporate investigations and insider threat mitigation will be shaped by the integration of advanced technologies, predictive analytics, and policy innovation. Emerging trends emphasize not only the importance of adaptive threat detection systems but also the necessity for forward-thinking governance structures, continuous learning, and a proactive security culture (Greenblott *et al*., 2019; Buhring and Koskinen, 2019). This explores key future directions and offers strategic recommendations for MNCs to enhance their resilience against insider threats.

Emerging technologies such as artificial intelligence (AI), machine learning (ML), behavioral analytics, and blockchain are transforming how insider threats are identified and investigated. AI-powered algorithms can detect anomalies in user behavior by analyzing vast amounts of data from email traffic, access logs, and communication platforms. Blockchain, on the other hand, offers immutable audit trails that ensure data integrity in investigative processes, strengthening evidence reliability. Additionally, natural language processing (NLP) is increasingly used in analyzing communications to detect intent or stress indicators. The convergence of these tools facilitates faster, more accurate

investigations while preserving data privacy and compliance standards.

Developing adaptive and predictive insider threat programs is essential for staying ahead of sophisticated threats. Traditional reactive models are increasingly inadequate. Instead, organizations must implement systems that learn and evolve based on new threat patterns. Predictive models integrate behavioral baselines with real-time risk scoring, enabling preemptive interventions. Adaptive programs should include dynamic risk profiles that adjust according to contextual factors such as organizational role changes, access privilege shifts, or regional geopolitical developments (Sarta *et al*., 2021; Hanelt *et al*., 2021). Incorporating feedback loops from past investigations into current threat models enhances their effectiveness over time.

Policy recommendations for multinational corporations should focus on harmonization, scalability, and inclusivity. First, establishing a globally consistent insider threat policy framework is essential, but it must be flexible enough to account for local legal, cultural, and regulatory differences. This includes defining acceptable monitoring practices, data handling protocols, and employee privacy safeguards. Second, companies should institutionalize cross-functional security governance by creating integrated risk committees that include representatives from IT, HR, compliance, and legal departments. Third, implementing a tiered policy model where core global policies are augmented by region-specific adaptations ensures coherence without sacrificing local relevance (Gopalakrishnan *et al*., 2020; Causa *et al*., 2021). Finally, MNCs should encourage public-private partnerships to share threat intelligence, foster innovation, and align with regulatory developments.

Continuous learning and improvement must become a cornerstone of insider threat mitigation. This involves not only post-incident reviews but also regular audits, training updates, and benchmarking against industry best practices. Learning systems both human and algorithmic must adapt to reflect the changing nature of threats. Organizations should invest in ongoing professional development, including certifications in investigative best practices, data privacy, and cross-cultural communication. Internal knowledge-sharing platforms and global security communities of practice can reinforce collective intelligence and accelerate learning curves across regions.

Moreover, fostering a culture of psychological safety and ethical conduct is equally critical. Employees must feel secure in reporting suspicious behavior without fear of retaliation. Anonymous reporting channels, clear whistleblower protections, and leadership commitment to transparency can encourage early detection and reduce the likelihood of insider misconduct. Continuous engagement through security awareness campaigns, gamified training, and feedback mechanisms can also reinforce vigilance and foster a shared responsibility for organizational security (Silic and Lowry, 2020; Sharif and Ameen, 2020)

The future of corporate investigations and insider threat mitigation in multinational corporations will be increasingly data-driven, adaptive, and collaborative. Emerging technologies will enable more precise and proactive threat detection, while adaptive risk models and harmonized policies will enhance global coherence. Leadership must prioritize continuous learning, cross-functional governance, and employee empowerment to build resilient, trustworthy, and secure enterprises. As insider threats become more complex and integrated with external influences, these strategic investments will be critical in sustaining organizational integrity and operational continuity.

3. Conclusion

The increasing complexity and transnational nature of insider threats in multinational corporations (MNCs) necessitate a strategic and dynamic response framework. A risk-based approach to corporate investigations emerges as a pivotal paradigm, enabling organizations to proactively identify, assess, and mitigate threats based on the likelihood of occurrence and potential impact. Unlike traditional, reactive models, this approach allows for a nuanced understanding of insider behavior within diverse operational and cultural contexts, ultimately supporting more targeted and effective intervention strategies.

For MNCs, the strategic implications of adopting a risk-based methodology are profound. First, it enables prioritization of investigative resources, ensuring attention is directed to high-risk areas and individuals. Second, it supports organizational resilience by embedding security considerations within broader governance, compliance, and business continuity frameworks. Third, it fosters agility in responding to evolving threat landscapes, especially when paired with real-time analytics, behavioral monitoring, and cross-functional collaboration. Furthermore, recognizing and accounting for regional variations legal, cultural, and regulatory ensures that corporate policies are both globally coherent and locally applicable.

To meet the demands of today's volatile threat environment, there is an urgent need for integrated, culturally informed, and leadership-driven investigative practices. Organizations must unify information security, human resources, legal, and operational departments under a cohesive investigative strategy that respects local nuances while aligning with global standards. Leadership plays a critical role in promoting transparency, trust, and accountability, which are essential for fostering a culture of security awareness. Ultimately, by embracing a risk-based, culturally competent, and leadership-centric approach to insider threat mitigation, multinational organizations can enhance their investigative efficacy, protect sensitive assets, and ensure long-term organizational integrity and sustainability.

4. References

1. Abayomi AA, Mgbame AC, Akpe OEE, Ogbuefi E, Adeyelu OO. Advancing equity through technology: Inclusive design of BI platforms for small businesses. IRE J. 2021;5(4):235-7. Available from: https://irejournals.com/paper-details/1708220
2. Abayomi AA, Ubanadu BC, Daraojimba AI, Agboola OA, Ogbuefi E, Owoade S. A conceptual framework for real-time data analytics and decision-making in cloud-optimized business intelligence systems. IRE J. 2021;4(9):271-2. Available from: https://irejournals.com/paper-details/1708317
3. Abisoye A, Akerele JI. High-Impact Data-Driven Decision-Making Model for Integrating Cutting-Edge Cybersecurity Strategies into Public Policy, Governance, and Organizational Frameworks. 2021.
4. Abisoye A, Akerele JI. A practical framework for advancing cybersecurity, artificial intelligence and technological ecosystems to support regional economic development and innovation. Int J Multidiscip Res

Growth Eval. 2022;3(1):700-13.
5. Abisoye A, Akerele JI. A scalable and impactful model for harnessing artificial intelligence and cybersecurity to revolutionize workforce development and empower marginalized youth. Int J Multidiscip Res Growth Eval. 2022;3(1):714-9.
6. Abisoye A. AI Literacy in STEM Education: Policy Strategies for Preparing the Future Workforce. 2023.
7. Abisoye A. Developing a Conceptual Framework for AI-Driven Curriculum Adaptation to Align with Emerging STEM Industry Demands. 2023.
8. Abisoye A, Udeh CA, Okonkwo CA. The Impact of AI-Powered Learning Tools on STEM Education Outcomes: A Policy Perspective. 2022.
9. Ochuba NA, Eyeregba ME, Onifade O, Ezeh FS. Advances in Automation of Administrative and Operational Processes Across Financial and Service-Based Organizations. Int J Manag Organ Res. 2022;1(1):159-64. doi:10.54660/IJMOR.2022.1.1.159-164
10. Adkins H, Beyer B, Blankinship P, Lewandowski P, Oprea A, Stubblefield A. Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems. O'Reilly Media; 2020.
11. Afolabi SO, Akinsooto O. Theoretical framework for dynamic mechanical analysis in material selection for high-performance engineering applications. Noûs. 2021;3.
12. Afolabi SO, Akinsooto O. Conceptual framework for mitigating cracking in superalloy structures during wire arc additive manufacturing (WAAM). Int J Multidiscip Compr Res. 2023. Available from: https://www.allmultidisciplinaryjournal.com/uploads/archives/20250123172459_MGE-2025-1-190.1.pdf
13. Ajayi SAO, Akanji OO. Impact of BMI and Menstrual Cycle Phases on Salivary Amylase: A Physiological and Biochemical Perspective. 2021.
14. Akinsooto O. Electrical Energy Savings Calculation in Single Phase Harmonic Distorted Systems [PhD thesis]. University of Johannesburg; 2013.
15. Akinsooto O, De Canha D, Pretorius JHC. Energy savings reporting and uncertainty in Measurement & Verification. In: 2014 Australasian Universities Power Engineering Conference (AUPEC). IEEE; 2014:1-5.
16. Akpe OEE, Kisina D, Adanigbo OS, Uzoka AC, Ochuba NA, Gbenle TP. A conceptual framework for building cost-conscious CI/CD workflows in agile software teams. Int J Manag Organ Res. 2023;2(2):135-42. doi:10.54660/IJMOR.2023.2.2.135-142
17. Akpe OEE, Kisina D, Owoade S, Uzoka AC, Ubanadu BC, Daraojimba AI. Systematic review of application modernization strategies using modular and service-oriented design principles. Int J Multidiscip Res Growth Eval. 2022;2(1):995-1001. doi:10.54660/IJMRGE.2022.2.1.995-1001
18. Akpe OEE, Mgbame AC, Ogbuefi E, Abayomi AA, Adeyelu OO. Bridging the business intelligence gap in small enterprises: A conceptual framework for scalable adoption. IRE J. 2020;4(2):159-61. Available from: https://irejournals.com/paper-details/1708222
19. Ali RF, Dominic PDD, Ali SEA, Rehman M, Sohail A. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Appl Sci. 2021;11(8):3383.
20. Attah JO, Mbakuuv SH, Ayange CD, Achive GW, Onoja VS, Kaya PB, *et al*. Comparative Recovery of Cellulose Pulp from Selected Agricultural Wastes in Nigeria to Mitigate Deforestation for Paper. Eur J Mater Sci. 2022;10(1):23-36.
21. Babun L, Denney K, Celik ZB, McDaniel P, Uluagac AS. A survey on IoT platforms: Communication, security, and privacy perspectives. Comput Netw. 2021;192:108040.
22. Bell AJ, Rogers MB, Pearce JM. The insider threat: Behavioral indicators and factors influencing likelihood of intervention. Int J Crit Infrastruct Prot. 2019;24:166-76.
23. Bergmann M, Schäpke N, Marg O, Stelzer F, Lang DJ, Bossert M, *et al*. Transdisciplinary sustainability research in real-world labs: success factors and methods for change. Sustain Sci. 2021;16:541-64.
24. Bernstein RS, Bulger M, Salipante P, Weisinger JY. From diversity to inclusion to equity: A theory of generative interactions. J Bus Ethics. 2020;167:395-410.
25. Birdi K, Griffiths K, Turgoose C, Alsina V, Andrei D, Băban A, *et al*. Factors influencing cross-border knowledge sharing by police organisations: an integration of ten European case studies. Police Pract Res. 2021;22(1):3-22.
26. Brass I, Sowell JH. Adaptive governance for the Internet of Things: Coping with emerging security risks. Regul Gov. 2021;15(4):1092-110.
27. Buhring J, Koskinen I. Beyond forecasting: a design-inspired foresight approach for preferable futures. Philos Frameworks Des Process. 2019;2:91.
28. Causa O, Abendschein M, Cavalleri MC. The laws of attraction: Economic drivers of inter-regional migration, housing costs and the role of policies. OECD Econ Dep Work Pap. 2021;(1679):1-68.
29. Esan OJ, Uzozie OT, Onaghinor O, Osho GO, Olatunde J. Leading with Lean Six Sigma and RPA in High-Volume Distribution: A Comprehensive Framework for Operational Excellence. 2023.
30. Eyeregba ME, Ochuba NA, Onifade O, Ezeh FS. A Conceptual Model for Cross-Functional Collaboration Between Finance and Program Teams in Grant-Based Projects. IRE J. 2021;4(7):174.
31. Eyeregba ME, Onifade O, Ezeh FS. Advances in Budgeting and Forecasting Models for Strategic Alignment in Financial and Nonprofit Organizations. IRE J. 2020;3(8):236.
32. Eyeregba ME, Onifade O, Ezeh FS. Systematic Review of Financial Operations and Oversight Mechanisms in Multi-Sectoral Organizational Structures. IRE J. 2020;3(7).
33. Ezeanochie CC, Afolabi SO, Akinsooto O. A Conceptual Model for Industry 4.0 Integration to Drive Digital Transformation in Renewable Energy Manufacturing. 2021.
34. Ezeanochie CC, Afolabi SO, Akinsooto O. Advancing Automation Frameworks for Safety and Compliance in Offshore Operations and Manufacturing Environments. 2022.
35. Festini SB, Katz B. A frontal account of false alarms. J Cogn Neurosci. 2021;33(9):1657-78.
36. Gopalakrishnan A, Zacharia PU, George G. Impact,

vulnerability and adaptation strategies for marine fisheries of India. 2020.
37. Greenblott JM, O'Farrell T, Olson R, Burchard B. Strategic foresight in the federal government: a survey of methods, resources, and institutional arrangements. World Futures Rev. 2019;11(3):245-66.
38. Hanelt A, Bohnsack R, Marz D, Antunes Marante C. A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. J Manag Stud. 2021;58(5):1159-97.
39. Hlanga MF. Regulatory Compliance of Electric Hot Water Heaters: A Case Study [PhD thesis]. University of Johannesburg; 2022.
40. Holt W, Dawson R, Agoro H. Development of an Automated Digital Forensics Toolkit for Incident Response. 2021.
41. Iyabode LC. Career Development and Talent Management in Banking Sector. Texila Int J. 2015.
42. Johnson GA, Martin S, Vanderslott S, Matuvanga TZ, Mavoko HM, Mulopo PM, *et al*. "People Are Not Taking the Outbreak Seriously": Interpretations of Religion and Public Health Policy During the COVID-19 Pandemic. In: *Caring on the Frontline during COVID-19: Contributions from Rapid Qualitative Research*. Springer; 2022:113-38.
43. Kalu A, Eyeregba ME, Ochuba NA, Onifade O, Ezeh FS. Advances in Strategic Dashboarding for Financial Performance Tracking in Nonprofit and Banking Institutions. Int J Soc Sci Except Res. 2023;2(1):256-61. doi:10.54660/IJSSER.2023.2.1.256-261
44. Kaul D, Khurana R. AI to detect and mitigate security vulnerabilities in APIs: encryption, authentication, and anomaly detection in enterprise-level distributed systems. Eigenpub Rev Sci Technol. 2021;5(1):34-62.
45. Khan AA, Uddin M, Shaikh AA, Laghari AA, Rajput AE. MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. IEEE Access. 2021;9:103637-50.
46. Khando K, Gao S, Islam SM, Salman A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. Comput Secur. 2021;106:102267.
47. Khatibi FS, Dedekorkut-Howes A, Howes M, Torabi E. Can public awareness, knowledge and engagement improve climate change adaptation policies?. Discov Sustain. 2021;2:1-24.
48. Kisina D, Akpe OEE, Ochuba NA, Ubanadu BC, Daraojimba AI, Adanigbo OS. Advances in backend optimization techniques using caching, load distribution, and response time reduction. IRE J. 2021;5(1):467-72. Available from: https://irejournals.com/paper-details/1708127
49. Kisina D, Akpe OEE, Owoade S, Ubanadu BC, Gbenle TP, Adanigbo OS. A conceptual framework for full-stack observability in modern distributed software systems. IRE J. 2021;4(10):293-8. Available from: https://irejournals.com/paper-details/1708126
50. Kisina D, Akpe OEE, Owoade S, Ubanadu BC, Gbenle TP, Adanigbo OS. A conceptual framework for implementing zero trust principles in cloud and hybrid IT environments. IRE J. 2022;5(8):412-7. Available from: https://irejournals.com/paper-details/1708124
51. Kisina D, Akpe OEE, Owoade S, Ubanadu BC, Gbenle TP, Adanigbo OS. Advances in continuous integration and deployment workflows across multi-team development pipelines. Int J Multidiscip Res Growth Eval. 2022;2(1):990-4. doi:10.54660/IJMRGE.2022.2.1.990-994
52. Kisina D, Ochuba NA, Owoade S, Uzoka AC, Gbenle TP, Adanigbo OS. A conceptual framework for scalable microservices in real-time airline operations platforms. IRE J. 2023;6(8):344-9. Available from: https://irejournals.com/paper-details/1708125
53. Knight E, Daymond J, Paroutis S. Design-led strategy: how to bring design thinking into the art of strategic management. Calif Manage Rev. 2020;62(2):30-52.
54. Lu J, Zhang Z, Jia M. Does servant leadership affect employees' emotional labor? A social information-processing perspective. J Bus Ethics. 2019;159(2):507-18.
55. Mgbame AC, Akpe OEE, Abayomi AA, Ogbuefi E, Adeyelu OO. Barriers and enablers of BI tool implementation in underserved SME communities. IRE J. 2020;3(7):211-3. Available from: https://irejournals.com/paper-details/1708221
56. Mgbame AC, Akpe OEE, Abayomi AA, Ogbuefi E, Adeyelu OO. Building data-driven resilience in small businesses: A framework for operational intelligence. IRE J. 2021;4(9):253-7. Available from: https://irejournals.com/paper-details/1708218
57. Nyame G, Qin Z. Precursors of role-based access control design in KMS: A conceptual framework. Information. 2020;11(6):334.
58. Ochuba NA, Onifade O, Eyeregba ME, Kalu A, Ezeh FS. Systematic Review of Change Management Strategies for Financial Transformation and Cost Efficiency Initiatives. Int J Soc Sci Except Res. 2023;2(1):292-8. doi:10.54660/IJSSER.2023.2.1.292-298
59. Ofori-Asenso R, Ogundipe O, Agyeman AA, Chin KL, Mazidi M, Ademi Z, *et al*. Cancer is associated with severe disease in COVID-19 patients: a systematic review and meta-analysis. Ecancermedicalscience. 2020;14:1047.
60. Ogbuefi E, Mgbame AC, Akpe OEE, Abayomi AA, Adeyelu OO. Affordable automation: Leveraging cloud-based BI systems for SME sustainability. IRE J. 2021;4(12):393-7. Available from: https://irejournals.com/paper-details/1708219
61. Ogeawuchi JC, Akpe OEE, Abayomi AA, Agboola OA, Ogbuefi E, Owoade S. Systematic review of advanced data governance strategies for securing cloud-based data warehouses and pipelines. IRE J. 2021;5(1):476-8. Available from: https://irejournals.com/paper-details/1708318
62. Ogundipe O, Mazidi M, Chin KL, Gor D, McGovern A, Sahle BW, *et al*. Real-world adherence, persistence, and in-class switching during use of dipeptidyl peptidase-4 inhibitors: a systematic review and meta-analysis involving 594,138 patients with type 2 diabetes. Acta Diabetol. 2021;58:39-46.
63. Ogundipe O, Sangoleye D, Udokanma E. "People Are Not Taking the Outbreak Seriously": Interpretations of Religion and Public Health Policy During. *Caring Frontline COVID-19*. 2022:113.
64. Omisola JO, Etukudoh EA, Okenwa OK, Tokunbo GI. Innovating Project Delivery and Piping Design for

Sustainability in the Oil and Gas Industry: A Conceptual Framework. Perception. 2020;24:28-35.
65. Onifade O, Eyeregba ME, Ezeh FS. A Conceptual Framework for Enhancing Grant Compliance through Digital Process Mapping and Visual Reporting Tools. IRE J. 2020;3(9).
66. Onifade O, Ochuba NA, Eyeregba ME, Kalu A, Ezeh FS. A Conceptual Framework for Unified Financial and Customer Data Management Using CRM and Planful Systems. Int J Soc Sci Except Res. 2023;2(1):249-55. doi:10.54660/IJSSER.2023.2.1.249-255
67. Onifade O, Ochuba NA, Eyeregba ME, Ezeh FS. Systematic Review of Requirements Gathering and Budget Governance in Public Sector and Nonprofit Project Management. Int J Multidiscip Res Growth Eval. 2021;2(1):902-8. doi:10.54660/.IJMRGE.2021.2.1.902-908
68. Onifade O, Ochuba NA, Eyeregba ME, Ezeh FS. Systematic Review of ROI-Focused Business Analysis Techniques for Budget Efficiency and Resource Allocation. Int J Manag Organ Res. 2022;1(1):165-70. doi:10.54660/IJMOR.2022.1.1.165-170
69. Puzis R, Zilberman P, Elovici Y. ATHAFI: Agile threat hunting and forensic investigation. arXiv. 2020. Preprint. Available from: https://arxiv.org/abs/2003.03663
70. Sarta A, Durand R, Vergne JP. Organizational adaptation. J Manag. 2021;47(1):43-75.
71. Saxena N, Hayes E, Bertino E, Ojo P, Choo KKR, Burnap P. Impact and key challenges of insider threats on organizations and critical businesses. Electronics. 2020;9(9):1460.
72. Sharif KH, Ameen SY. A review of security awareness approaches with special emphasis on gamification. In: 2020 International Conference on Advanced Science and Engineering (ICOASE). IEEE; 2020:151-6.
73. Sheikh A, Anderson M, Albala S, Casadei B, Franklin BD, Richards M, *et al*. Health information technology and digital innovation for national learning health and care systems. Lancet Digit Health. 2021;3(6):e383-96.
74. Silic M, Lowry PB. Using design-science based gamification to improve organizational security training and compliance. J Manag Inf Syst. 2020;37(1):129-61.
75. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun Surv Tutor. 2020;22(2):1191-221.
76. Tasleem N, Gangadharan S. Navigating stakeholder dynamics in large-scale transformations. J Adv Multidiscip Res. 2022;1(2):48-56.
77. Tang X. Chinese manufacturing investments and knowledge transfer: A report from Ethiopia. SAIS-CARI Work Pap. 2019;3.
78. Uddin M, Islam S, Al-Nemrat A. A dynamic access control model using authorising workflow and task-role-based access control. IEEE Access. 2019;7:166676-89.
79. Varga S, Brynielsson J, Franke U. Cyber-threat perception and risk management in the Swedish financial sector. Comput Secur. 2021;105:102239.
80. Vindrola-Padros C, Johnson GA. *Caring on the Frontline during COVID-19*. Springer; 2022.
81. Zelenay J, Balco P, Greguš M. Cloud technologies-solution for secure communication and collaboration. Procedia Comput Sci. 2019;151:567-74.
82. Zhang Y. Mitigating Insider Threats in Enterprise Storage Systems: A Security Framework for Data Integrity and Access Control. Int J Trend Sci Res Dev. 2020;4(4):1878-90.