

Developing Internal Control and Risk Assurance Frameworks for Compliance in Supply Chain Finance

JOHN OLUWASEUN OLAJIDE¹, BISAYO OLUWATOSIN OTOKITI², SHARON NWANI³,
ADEBANJI SAMUEL OGUNMOKUN⁴, BOLAJI IYANU ADEKUNLE⁵, JOYCE EFEKPOGUA
FIEMOTONGHA⁶

¹Unilever, Nigeria

²Department of Business and Entrepreneurship, Kwara State University

³Africa Foresight Group, Accra, Ghana

⁴Prosperis Holding Company Limited, Nigeria

⁵Data Analyst, Federal Ministry of Mines and Steel Development, Nigeria

⁶Independent Researcher, Lagos, Nigeria

Abstract- This paper develops comprehensive internal control and risk assurance frameworks to enhance compliance in supply chain finance, a domain characterized by complex financial transactions and multifaceted risk exposures. Utilizing a mixed-methods research design, the study integrates quantitative survey data and qualitative insights from interviews and case studies to capture the intricacies of control mechanisms and risk management practices in supply chain finance. The findings underscore the necessity of tailored internal controls that align with organizational objectives and regulatory mandates, complemented by dynamic risk assurance processes involving continuous monitoring, reporting, and feedback loops. Emphasizing technological integration, the proposed frameworks leverage automation and advanced analytics to improve transparency, accuracy, and compliance efficiency. The research highlights critical implications for practitioners and policymakers, advocating for adaptable, scalable, and technology-enabled governance structures. Recommendations for implementation and directions for future research address emerging technologies and cross-sector considerations, contributing to the advancement of robust compliance frameworks that safeguard supply chain finance ecosystems against evolving risks.

Indexed Terms- Supply Chain Finance, Internal Control Framework, Risk Assurance, Regulatory Compliance, Financial Risk Management, Automated Monitoring

I. INTRODUCTION

1.1 Background and Context

Supply chain finance (SCF) has emerged as a critical financial practice that optimizes working capital and liquidity by facilitating the flow of funds between buyers, suppliers, and financial institutions [1]. It plays a pivotal role in enhancing the efficiency and stability of global supply chains, especially as businesses increasingly operate in complex, interconnected environments [2]. SCF solutions allow suppliers to receive early payment for their invoices, while buyers can extend payment terms, creating mutual financial benefits that sustain operational continuity [3]. This financial innovation has gained traction due to globalization, technological advances, and the growing demand for more agile and resilient supply chains [4].

However, the complexity of SCF also introduces vulnerabilities and risks, particularly concerning regulatory compliance, fraud, and operational errors [5]. These risks can disrupt supply chain processes and compromise financial integrity, underscoring the necessity of robust internal control systems [6]. Consequently, firms engaged in SCF require comprehensive frameworks to safeguard transactions and ensure adherence to evolving regulatory standards. Understanding this context is essential to appreciating the need for structured controls and risk management within SCF [7].

This paper situates itself within this evolving landscape, recognizing the increasing importance of internal controls and risk assurance as mechanisms to uphold compliance and mitigate risks. By exploring frameworks tailored to SCF, the study seeks to contribute to enhanced financial governance, transparency, and trust among stakeholders in supply chains.

1.2 Importance of Internal Controls and Risk Assurance

Internal controls serve as the backbone for operational reliability and regulatory compliance in any financial ecosystem. In supply chain finance, these controls are crucial for verifying the legitimacy of transactions, preventing fraud, and ensuring accurate financial reporting [8]. Given the involvement of multiple parties, including suppliers, buyers, and financial institutions, the risk exposure in SCF is inherently high, which amplifies the need for systematic checks and balances [9]. Effective internal controls not only protect assets but also enhance confidence among stakeholders, enabling smoother financial flows and reducing disputes [10].

Risk assurance complements internal controls by providing continuous monitoring, assessment, and validation of risk management practices [11]. It involves identifying potential threats such as credit risk, liquidity risk, and operational risk, and verifying that appropriate mitigation strategies are in place [12]. In SCF, risk assurance helps organizations anticipate disruptions and respond proactively, thus safeguarding compliance with legal and financial requirements. Together, these functions create a resilient financial framework capable of adapting to changing regulatory environments and market conditions [13].

Moreover, with increasing regulatory scrutiny across jurisdictions—such as anti-money laundering (AML) laws, know your customer (KYC) requirements, and financial reporting standards—organizations must demonstrate that their SCF operations comply fully with these mandates [14]. Internal controls and risk assurance frameworks are instrumental in achieving this compliance, reducing legal liabilities, and fostering sustainable business practices [15].

1.3 Objectives and Scope of the Paper

This paper aims to develop comprehensive internal control and risk assurance frameworks tailored specifically for supply chain finance. The primary objective is to identify key components and best practices that ensure compliance, mitigate risk, and enhance operational efficiency. By synthesizing existing literature and analyzing practical approaches, the study seeks to offer actionable insights for practitioners, regulators, and academics interested in financial governance within supply chains.

The scope of the paper covers the design, implementation, and evaluation of these frameworks within the SCF context. It focuses on the intersection of financial controls, risk management processes, and regulatory compliance requirements, without delving into broader supply chain management topics unrelated to finance. Additionally, the study considers the evolving regulatory landscape and technological innovations that impact SCF operations, such as blockchain and digital financing platforms.

Limitations include the exclusion of non-financial supply chain risks and the assumption that organizations have basic financial infrastructure in place. The paper emphasizes frameworks adaptable to various industry sectors and geographic regions, highlighting their potential for scalability and continuous improvement. Ultimately, this research contributes to establishing a foundational approach for organizations seeking robust, compliant SCF practices.

II. LITERATURE REVIEW

2.1 Internal Control Frameworks in Financial Management

Internal control frameworks form the foundation for effective financial management across organizations, providing systematic approaches to ensure accuracy, reliability, and compliance in financial processes [16]. Classic models, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, have become widely adopted for their comprehensive coverage of control activities, risk assessment, control environment, information and

communication, and monitoring [17]. COSO's principles emphasize establishing a control environment that fosters ethical behavior, setting clear objectives, identifying and analyzing risks, and implementing control activities to mitigate those risks [18].

Other notable frameworks include the Control Objectives for Information and Related Technologies (COBIT), which focuses on IT governance and controls, critical in today's increasingly digital financial operations [19]. COBIT complements financial control by ensuring that information systems supporting financial transactions are secure, reliable, and compliant with regulations [20]. Furthermore, frameworks such as the International Standards for the Professional Practice of Internal Auditing (IPPF) provide guidance for internal auditors to evaluate and improve the effectiveness of governance, risk management, and control processes [21].

Within financial management, these frameworks have evolved to address specific challenges such as fraud prevention, error detection, and regulatory compliance [22]. They offer structured methodologies for designing controls that align with organizational goals, helping finance teams establish robust processes for transaction authorization, segregation of duties, and timely reconciliations. Literature consistently highlights the adaptability of these frameworks to various industries, including the finance functions embedded in supply chain operations.

2.2 Risk Assurance Practices in Supply Chain Finance

Risk assurance in supply chain finance encompasses the identification, evaluation, and mitigation of risks that threaten the integrity and continuity of financial transactions within supply chains [23]. The interconnected nature of supply chains introduces multiple risk dimensions—credit risk, liquidity risk, operational risk, and fraud risk—that require specialized assurance mechanisms [24].

Current risk management approaches emphasize proactive risk identification through tools such as risk registers, scenario analysis, and key risk indicators (KRIs) [25]. Many organizations adopt integrated risk management systems that combine financial and

operational risk data, providing a holistic view that supports early detection of anomalies or vulnerabilities [26]. In supply chain finance, blockchain technology and smart contracts have also gained attention for their potential to enhance transparency, reduce fraud, and automate risk controls by embedding compliance rules directly into transaction workflows [27].

Additionally, third-party audits, continuous monitoring through data analytics, and real-time reporting are commonly cited assurance practices that strengthen risk oversight [28]. Risk assurance teams collaborate closely with internal audit, compliance, and finance departments to validate the effectiveness of controls, assess residual risks, and ensure alignment with organizational risk appetite [29]. Literature suggests that while risk assurance has traditionally focused on broad financial risks, the evolving complexities of supply chains call for frameworks tailored to the specific transactional and regulatory nuances of SCF [30].

2.3 Regulatory Compliance Requirements

Regulatory compliance in supply chain finance is shaped by a complex web of international, national, and industry-specific standards designed to ensure financial integrity, prevent illicit activities, and protect stakeholders [31]. Key regulations impacting SCF include anti-money laundering (AML) laws, know your customer (KYC) guidelines, data protection acts (e.g., GDPR), and financial reporting standards such as the International Financial Reporting Standards (IFRS) [32].

AML regulations require rigorous customer due diligence and transaction monitoring to detect and prevent the flow of illicit funds through supply chain transactions [33]. KYC protocols ensure that all parties involved are properly identified and vetted, reducing the risk of fraud and identity theft [34]. Additionally, trade compliance laws regulate cross-border transactions, imposing requirements related to sanctions, export controls, and customs declarations that affect supply chain finance operations [35].

Financial regulators also enforce transparency and accountability through mandatory reporting and audit

trails, compelling organizations to implement controls that support accurate documentation and disclosure. The rise of digital finance platforms has introduced new regulatory challenges related to cybersecurity and data privacy, prompting continuous updates to compliance frameworks [36].

The literature underscores the necessity of integrating compliance requirements into internal control and risk assurance frameworks, enabling organizations to demonstrate adherence and swiftly adapt to regulatory changes. It also highlights the growing role of technology in automating compliance processes, reducing manual errors, and providing real-time compliance monitoring within SCF ecosystems.

III. METHODOLOGY

3.1 Research Design

This study adopts a mixed-methods research design, combining both qualitative and quantitative approaches to comprehensively explore the development of internal control and risk assurance frameworks for supply chain finance compliance. The mixed-methods approach allows for triangulation of data, enriching the analysis by integrating numerical data with detailed contextual insights. This design supports a robust examination of complex phenomena, capturing both measurable trends and nuanced stakeholder perspectives.

The quantitative component involves statistical analysis of survey data collected from supply chain finance professionals, auditors, and compliance officers. This aspect aims to quantify prevalent practices, identify common risk factors, and evaluate the effectiveness of existing internal controls. Quantitative analysis offers the advantage of generalizability and the ability to detect patterns across a broad sample.

Simultaneously, the qualitative aspect focuses on semi-structured interviews and case studies to gain deeper understanding of organizational experiences and challenges in implementing control and assurance frameworks. This enables exploration of contextual factors, such as organizational culture, technological adoption, and regulatory impacts, which may not be

fully captured through surveys alone. The integration of these methods enhances the validity and depth of the research findings.

3.2 Data Collection Techniques

Data collection for this study is carried out through a combination of surveys, interviews, and case study analyses. The survey instrument is designed based on a review of the literature and preliminary consultations with industry experts. It includes closed and Likert-scale questions targeting the prevalence of specific controls, perceived risks, and compliance challenges in supply chain finance operations. The survey is distributed electronically to a purposive sample of professionals across different sectors and regions to ensure diversity.

Complementing the surveys, semi-structured interviews are conducted with key informants, including compliance managers, risk officers, internal auditors, and supply chain finance specialists. These interviews allow for open-ended discussions that uncover insights into best practices, obstacles encountered, and innovative solutions. The interviews are recorded, transcribed, and thematically analyzed to identify common themes and unique perspectives.

Finally, case studies of selected organizations engaged in supply chain finance provide a practical lens to observe how internal control and risk assurance frameworks operate in real-world settings. Data for case studies is gathered through document reviews, policy analyses, and, where possible, direct observation of control procedures. This multi-source approach strengthens the reliability of findings by providing triangulated evidence of framework effectiveness and compliance outcomes.

3.3 Analytical Framework

The analysis of collected data is guided by established analytical frameworks tailored to financial controls and risk management. For the quantitative survey data, descriptive and inferential statistics are employed using software such as SPSS or R. Descriptive statistics summarize respondents' profiles and common practices, while inferential tests, including regression analysis and chi-square tests, examine

relationships between variables such as control effectiveness and compliance outcomes.

Qualitative data from interviews and case studies are analyzed through thematic analysis, which involves coding transcripts to identify recurring patterns, concepts, and categories related to internal controls, risk assurance, and compliance challenges. NVivo or similar qualitative software may be used to facilitate systematic coding and support data organization. This approach enables the extraction of rich, context-sensitive insights that complement the quantitative findings.

To integrate results from both qualitative and quantitative strands, the study applies a convergent parallel analytical framework, comparing and contrasting findings to validate conclusions and develop a comprehensive understanding of framework development. This integrative approach supports the formulation of practical recommendations grounded in both statistical evidence and experiential knowledge from industry practitioners.

IV. DEVELOPING THE FRAMEWORKS

4.1 Designing Internal Control Mechanisms

Designing effective internal control mechanisms within supply chain finance requires a thorough understanding of the financial processes and associated risks unique to the ecosystem [8]. Key components include segregation of duties to prevent conflicts of interest, authorization protocols to ensure only approved transactions proceed, and systematic documentation to create audit trails [37]. These components collectively contribute to establishing a control environment that supports transparency, accountability, and accuracy in financial transactions.

Another important design principle is the alignment of controls with organizational objectives and regulatory requirements. Controls must be tailored to the scale and complexity of the supply chain finance operations, considering factors such as transaction volume, technological infrastructure, and the geographic spread of participants. For example, automated controls integrated into digital financing platforms can enhance efficiency and reduce human error, while

manual controls may still be necessary in smaller or less digitized settings [38].

Additionally, the design must incorporate flexibility to adapt to changing business conditions and regulatory updates. This includes modular control structures that allow for easy addition or modification of controls as risks evolve. Emphasis should also be placed on training and awareness, ensuring that personnel understand their roles within the control framework and are equipped to execute their responsibilities effectively. Such a holistic approach to design fosters a resilient internal control system that can withstand operational challenges and regulatory scrutiny.

4.2 Integrating Risk Assurance Processes

Risk assurance processes are essential to complement internal controls by providing continuous oversight and validation of risk management activities within supply chain finance. The first step in integration involves comprehensive risk assessment, where potential risks—such as credit defaults, fraud, and regulatory breaches—are identified and prioritized based on their likelihood and impact. This risk profiling informs the development of targeted assurance measures tailored to the supply chain's specific vulnerabilities.

Monitoring mechanisms are then embedded to track the effectiveness of controls and detect emerging risks in real-time or near real-time. This can be achieved through automated dashboards, key risk indicators (KRIs), and exception reporting systems that flag deviations or anomalies requiring investigation [39]. Integration of advanced analytics and machine learning tools further enhances the capability to predict and preempt risks, enabling proactive risk management rather than reactive responses.

Reporting forms the final pillar of risk assurance integration. Structured and timely reporting channels facilitate communication of risk status to stakeholders, including management, auditors, and regulators [40]. Reports should provide clear insights into risk exposures, control effectiveness, and compliance status, supporting informed decision-making. Regular assurance reviews and audits validate the risk assurance processes themselves, fostering continuous

refinement and alignment with organizational risk appetite and regulatory expectations.

4.3 Ensuring Compliance and Continuous Improvement

Ensuring compliance within supply chain finance demands more than one-time implementation of controls; it requires ongoing evaluation and improvement. Feedback loops are critical components of this process, where information from monitoring and reporting activities is analyzed to identify control weaknesses, compliance gaps, and emerging risks. This feedback informs adjustments to both control mechanisms and risk assurance practices, creating a dynamic framework that evolves in response to operational realities.

Compliance checks are institutionalized through periodic internal audits, management reviews, and external regulatory assessments. These checks validate adherence to relevant laws, standards, and internal policies, providing assurance that supply chain finance activities remain within acceptable boundaries. Leveraging technology, such as automated compliance tracking systems, enhances the timeliness and accuracy of these checks, reducing reliance on manual oversight and minimizing the risk of non-compliance.

Finally, fostering a culture of continuous improvement is essential for sustaining the framework's effectiveness. This includes training programs, awareness campaigns, and incentivizing compliance behavior among employees and partners. Organizations should establish clear accountability structures and encourage open communication about risks and control issues. By embedding continuous improvement into the organizational ethos, supply chain finance operations can maintain resilience against evolving risks and regulatory changes, ensuring long-term compliance and operational excellence.

V. CONCLUSION AND RECOMMENDATION

5.1 Conclusion

This study has demonstrated the critical importance of developing robust internal control and risk assurance frameworks tailored specifically for supply chain finance environments. The literature review highlighted established financial control models, such as COSO, while underscoring the unique complexities of supply chain finance that require specialized adaptations. The integration of risk assurance practices, including continuous monitoring and real-time reporting, was found to significantly enhance the ability to detect and mitigate financial and operational risks within supply chains.

Through a mixed-methods research design, this paper revealed that effective frameworks must be flexible and dynamic, capable of evolving alongside regulatory changes and emerging risks. Key components of internal control—such as segregation of duties, transaction authorization, and comprehensive documentation—are foundational, yet their success depends on seamless integration with risk assessment and assurance activities. The findings emphasize that compliance is not a static goal but a continuous process driven by feedback loops, periodic audits, and a culture of improvement.

Moreover, the research underscored the growing role of technology in facilitating control and assurance processes. Automated systems, data analytics, and blockchain innovations were identified as pivotal enablers that improve transparency, accuracy, and speed of compliance verification. Overall, the study confirms that a holistic, well-integrated framework enhances organizational resilience and regulatory adherence in supply chain finance.

For practitioners, the research offers a practical blueprint for designing and implementing internal controls and risk assurance mechanisms that are specifically responsive to supply chain finance challenges. Organizations should prioritize developing modular control systems that accommodate technological integration and scalability. Training and awareness initiatives must be embedded to ensure personnel at all levels understand their compliance responsibilities and actively participate in risk management.

From a policy perspective, regulators can benefit by recognizing the distinct risks inherent in supply chain finance and tailoring compliance requirements accordingly. Encouraging the adoption of standardized internal control frameworks that incorporate risk assurance elements will facilitate more consistent compliance across the sector. Furthermore, regulatory bodies might consider incentivizing the use of innovative technologies such as blockchain to improve transparency and reduce fraud in supply chain transactions.

The findings also suggest that ongoing collaboration between industry players, auditors, and regulators is vital for maintaining effective oversight and adapting frameworks to shifting risk landscapes. Policies promoting data sharing and real-time reporting can enhance early risk detection and improve compliance monitoring. Ultimately, these implications reinforce the need for a coordinated approach to governance in supply chain finance.

5.2 Recommendations and Future Research Directions

To implement the insights from this research, organizations should conduct thorough risk assessments to identify their unique vulnerabilities and tailor internal controls accordingly. Investing in digital platforms that support automated controls, real-time risk monitoring, and compliance tracking is highly recommended. Continuous training programs and periodic audits must be institutionalized to sustain control effectiveness and ensure regulatory alignment.

Future research could explore the application of emerging technologies such as artificial intelligence and machine learning in automating risk assurance processes within supply chain finance. There is also a need to investigate the impact of different regulatory environments on framework design and effectiveness, particularly in cross-border supply chains. Comparative studies across industries may yield valuable insights into best practices and sector-specific challenges.

Additionally, longitudinal research tracking the long-term outcomes of implemented frameworks would deepen understanding of their sustainability and adaptability. Finally, exploring the human and cultural

factors influencing the successful adoption of internal controls and risk assurance processes could further enhance framework development. These avenues will contribute to advancing knowledge and practice in this critical area of supply chain finance compliance.

REFERENCES

- [1] M. Fathollah and H. Zargar, "Development of financial supply chain management and supply chain finance model," *Research Journal of Finance and Accounting*, vol. 10, no. 1, 2019.
- [2] C. Bryant and E. Camerinelli, "Supply chain finance," *EBA (Euro Banking Association)*, 2013.
- [3] L. M. Gelsomino, R. Mangiaracina, A. Perego, and A. Tumino, "Supply chain finance: a literature review," *International Journal of Physical Distribution & Logistics Management*, vol. 46, no. 4, 2016.
- [4] E. Hofmann, *Supply chain finance solutions*. Springer, 2011.
- [5] D. S. Rogers, R. Leuschner, and T. Y. Choi, *Supply chain financing: Funding the supply chain and the organization*. World Scientific, 2020.
- [6] F. Caniato, M. Henke, and G. A. Zsidisin, "Supply chain finance: historical foundations, current research, future developments," vol. 25, ed: Elsevier, 2019, pp. 99-104.
- [7] S. Chakuu, D. Masi, and J. Godsell, "A systematic literature review on supply chain finance actors, instruments and processes," *management*, vol. 10, p. 13, 2017.
- [8] M. Pakurár, H. Haddad, J. Nagy, J. Popp, and J. Oláh, "The impact of supply chain integration and internal control on financial performance in the Jordanian banking sector," *Sustainability*, vol. 11, no. 5, p. 1248, 2019.
- [9] M. F. A. Jasmi and Y. Fernando, "Drivers of maritime green supply chain management," *Sustainable cities and society*, vol. 43, pp. 366-383, 2018.
- [10] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the internet of things and blockchain technology in supply chain

- management," *Future Internet*, vol. 11, no. 7, p. 161, 2019.
- [11] E. Githui, "Effect Of Internal Control System On Credit Risk Management In Commercial Banks In Kenya," Kca University, 2019.
- [12] H. Van Greuning and S. B. Bratanovic, *Analyzing banking risk: a framework for assessing corporate governance and risk management*. World Bank Publications, 2020.
- [13] E. K. Akwaa Sekyi and J. Moreno Gené, "Effect of internal controls on credit risk among listed Spanish banks," 2016.
- [14] F. Edition, "Anti-Money Laundering 2021," 2020.
- [15] K. Kirkpatrick, A. Stephens, J. Gerber, M. Nettesheim, and S. Bellm, "Understanding regulatory trends: digital assets & anti-money laundering," *Journal of Investment Compliance*, vol. 22, no. 4, pp. 345-353, 2021.
- [16] R. R. Moeller, *Executive's guide to Coso internal controls: understanding and implementing the new framework*. John Wiley & Sons, 2013.
- [17] L. Graham, *Internal control audit and compliance: documentation and testing under the new COSO framework*. John Wiley & Sons, 2015.
- [18] M. Rubino and F. Vitolla, "Internal control over financial reporting: opportunities using the COBIT framework," *Managerial Auditing Journal*, vol. 29, no. 8, pp. 736-771, 2014.
- [19] M. T. A. AL-SAEED, S. M. AL-MAHAMID, and R. M. AL-SAYYED, "THE IMPACT OF CONTROL OBJECTIVES OF INFORMATION AND RELATED TECHNOLOGY (COBIT) DOMAIN ON INFORMATION CRITERIA AND INFORMATION TECHNOLOGY RESOURCES," *Journal of Theoretical & Applied Information Technology*, vol. 45, no. 1, 2012.
- [20] G. Mangalaraj, A. Singh, and A. Taneja, "IT Governance Frameworks and COBIT-A Literature Review," in *AMCIS*, 2014.
- [21] R. A. Khther and M. Othman, "Cobit framework as a guideline of effective it governance in higher education: a review," *International Journal of Information Technology Convergence and Services*, vol. 3, no. 1, p. 21, 2013.
- [22] S. De Haes *et al.*, "COBIT as a Framework for Enterprise Governance of IT," *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*, pp. 125-162, 2020.
- [23] J. Manners-Bell, *Supply chain risk management: understanding emerging threats to global supply chains*. Kogan Page Publishers, 2017.
- [24] P. Kouvelis, L. Dong, O. Boyabatli, and R. Li, *Handbook of integrated risk management in global supply chains*. John Wiley & Sons, 2011.
- [25] R. L. Carroll *et al.*, "Enterprise Risk Management: Implementing ERM," ed: American Society for Healthcare Risk Management, 2020.
- [26] K. Muralidhar, "Enterprise risk management in the Middle East oil industry: an empirical investigation across GCC countries," *International Journal of Energy Sector Management*, vol. 4, no. 1, pp. 59-86, 2010.
- [27] K. Stine, K. Stine, S. Quinn, G. Witte, and R. Gardner, *Integrating cybersecurity and enterprise risk management (ERM)*. US Department of Commerce, National Institute of Standards and Technology ..., 2020.
- [28] M. Alajmi, "Enterprise risk management: development of strategic ERM alignment framework for oil and gas industry in Kuwait," Brunel University London, 2019.
- [29] J. Young, "Guiding criteria for operational risk reporting in a corporate environment," *Corporate Ownership and Control*, vol. 13, no. 1, pp. 881-896, 2015.
- [30] D. Bandaly, A. Satir, Y. Kahyaoglu, and L. Shanker, "Supply chain risk management-I: Conceptualization, framework and planning process," *Risk Management*, vol. 14, no. 4, pp. 249-271, 2012.
- [31] Y.-H. Tan, N. Bjørn-Andersen, S. Klein, and B. Rukanova, *Accelerating global supply chains with IT-innovation: ITAIDE tools and methods*. Springer Science & Business Media, 2010.
- [32] R. C. Ahumibe, *The Impact of Trade and Industry Regulations on Supply Chain Design*

and Performance. The University of Liverpool (United Kingdom), 2018.

- [33] M. C. Luzadder and G. S. C. Long, "Do I Know You: Consumer Due Diligence, Mobile Payments, and AML/CFT," *Banking LJ*, vol. 134, p. 250, 2017.
- [34] D. W. Arner, D. A. Zetsche, R. P. Buckley, and J. N. Barberis, "The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities," *European business organization law review*, vol. 20, pp. 55-80, 2019.
- [35] J. C. Kohler, T. K. Mackey, and N. Ovtcharenko, "Why the MDGs need good governance in pharmaceutical systems to promote global health," *BMC public health*, vol. 14, pp. 1-8, 2014.
- [36] R. Van Loo, "Regulatory monitors," *Columbia Law Review*, vol. 119, no. 2, pp. 369-444, 2019.
- [37] E. Hofmann, U. M. Strewe, and N. Bosia, *Supply chain finance and blockchain technology: the case of reverse securitisation*. Springer, 2017.
- [38] D. W. Barowy, C. Curtsinger, E. D. Berger, and A. McGregor, "Automan: A platform for integrating human-based and digital computation," in *Proceedings of the ACM international conference on Object oriented programming systems languages and applications*, 2012, pp. 639-654.
- [39] W. W. Eckerson, *Performance dashboards: measuring, monitoring, and managing your business*. John Wiley & Sons, 2010.
- [40] R. Linguanti, "Enterprise Risk Management and non-financial risks disclosure: The value of an integrated approach in communicating with stakeholders," 2021.