A Review of Integrated Data and Compliance Systems for Strengthening Financial Transparency

MICHAEL UZOMA AGU[1], OLAWOLE AKOMOLAFE[2]
[1]*Shell Petroleum Development Company of Nigeria Limited*
[2]*Nigeria Liability Insurance Pool, Lagos, Nigeria*

Abstract- ***Financial transparency has become a critical component of global financial governance, influencing regulatory compliance, corporate accountability, and the stability of financial markets. As financial transactions, reporting processes, and compliance requirements grow increasingly complex, institutions have sought to integrate data systems, compliance tools, and analytical technologies to improve oversight and transparency. Prior to 2018, significant progress was made in developing data integration architectures, automated compliance mechanisms, and risk-based monitoring tools, yet fragmentation, inconsistent implementation, and uneven regulatory harmonisation impeded full realisation of their benefits. This paper reviews scholarly and regulatory literature on integrated data systems, compliance frameworks, financial reporting technologies, and data-governance practices that enhance transparency. It examines the evolution of integrated financial information systems, regulatory technology (RegTech), automated reporting tools, data-quality mechanisms, and cross-border compliance infrastructures. The review synthesises key developments, identifies challenges, and outlines conceptual pathways for strengthening transparency through integrated data-compliance ecosystems.***

Keywords: Financial Transparency; Integrated Data Systems; Compliance Management; Regtech; Data Governance; Financial Regulation

I. INTRODUCTION

Financial transparency is widely recognised as a cornerstone of effective financial governance, investor protection, and market integrity [1], [2]. In both public and private financial systems, transparency reduces information asymmetry, mitigates fraud, enhances accountability, and enables regulators to monitor risks more effectively [3], [4]. Prior to 2018, the rapid expansion of digital financial activities, globalised capital flows, and complex intermediation structures placed mounting pressure on institutions to adopt more sophisticated mechanisms for managing data, monitoring compliance, and reporting financial information [5], [6]. Traditional compliance frameworks largely manual, fragmented across departments, or reliant on disparate information systems proved increasingly inadequate for meeting the demands of contemporary financial oversight [7], [8]. As a result, organisations and regulatory bodies began placing greater emphasis on integrated data and compliance systems capable of consolidating information flows, standardising reporting formats, automating monitoring tasks, and supporting timely analysis of financial activities [9], [10].

The drive toward integrated data-compliance systems emerged in response to a series of structural developments in financial markets [11], [12]. First, the exponential growth of digital transactions generated unprecedented volumes of data, ranging from customer identification records and account histories to complex derivatives exposures and cross-border financial transfers. Financial institutions found themselves managing large, heterogeneous datasets spread across multiple business units and technology platforms [13], [14]. The inability to consolidate these data sources not only constrained operational efficiency but also hindered regulatory reporting, risk assessment, and internal audit processes. Integrated data systems promised to remedy these challenges by harmonising disparate databases into unified architectures capable of supporting enterprise-wide transparency [15], [16].

Second, the regulatory landscape evolved significantly in the years leading up to 2018. Major regulatory reforms including anti-money laundering (AML) directives, know-your-customer (KYC) requirements,

Basel III capital and liquidity standards, and international financial reporting regulations expanded the volume, granularity, and frequency of required disclosures. Regulatory authorities increasingly expected institutions to demonstrate traceability, data integrity, and timely compliance [17], [18]. Non-compliance risks escalated sharply, highlighted by growing financial penalties imposed on institutions for reporting inaccuracies, weak controls, and ineffective data management practices. These enforcement actions reinforced the importance of automated compliance systems, robust data-quality controls, and integrated reporting infrastructures capable of producing accurate regulatory submissions [19], [20].

Third, technological advances in data analytics, enterprise information systems, and workflow automation influenced organisational perspectives on transparency and compliance. Before 2018, institutions began adopting early forms of regulatory technology (RegTech) to streamline compliance tasks, automate transaction monitoring, and support real-time reconciliation and reporting. Although RegTech was not yet fully mature, its early applications demonstrated the potential of integrated data-compliance ecosystems to enhance the speed, consistency, and accuracy of financial oversight. These innovations encouraged organisations to rethink the architecture of compliance systems, moving away from siloed, manually intensive processes and toward holistic platforms that integrate data collection, analysis, and reporting [21], [22].

A central challenge, however, was the persistent fragmentation of financial data environments. Many institutions maintained legacy systems that lacked interoperability, used inconsistent data definitions, or produced incompatible reporting formats [23], [24]. As financial activities expanded across multiple digital channels, subsidiaries, and jurisdictional boundaries, institutions often struggled to maintain transparency across organisational structures [25], [26]. Data quality issues including inconsistencies, errors, incomplete records, and duplicated information further compromised transparency [27], [28]. Integrated data governance frameworks became increasingly essential, emphasising global data standards, metadata management, standardised taxonomies, and consistent reporting architectures [29], [30].

Moreover, the pressure for transparency extended beyond compliance obligations. Investors, analysts, customers, and civil society groups increasingly demanded greater access to reliable financial information [31], [32]. Events such as the 2008 financial crisis exposed weaknesses in risk reporting, balance-sheet transparency, and internal control systems. Subsequent failures in corporate governance, accounting fraud cases, and cross-border money-laundering operations further highlighted the inadequacy of conventional transparency mechanisms. Integrated data-compliance systems thus emerged as tools not only for meeting regulatory obligations but also for strengthening public trust and reinforcing ethical financial behaviour [33], [34].

An additional dimension stems from the globalisation of financial activities. Financial institutions with multinational operations face multiple, often inconsistent regulatory requirements [35], [36]. The lack of harmonised data standards and reporting expectations across jurisdictions increases the complexity of compliance. Integrated systems support cross-border transparency by consolidating geographically dispersed data into standardised structures that facilitate unified analysis and reporting [37], [38]. This capability enhances both institutional compliance and the capacity of regulatory bodies to conduct international supervisory cooperation [39].

Notably, integrated data-compliance ecosystems also contribute to stronger risk management. Transparency plays a crucial role in identifying emerging risks, detecting anomalies, understanding exposure concentrations, and supporting robust stress testing [40]. Without accurate and integrated data, risk models are compromised, internal controls are weakened, and the ability to respond to financial shocks is diminished [41], [42]. Through automated monitoring, centralised data warehousing, and rule-based compliance engines, integrated systems allow institutions to identify suspicious transactions, detect unusual behaviour, and monitor compliance breaches in real time. This supports preventive rather than reactive approaches to governance [43].

Despite these advances, institutions encountered substantial obstacles in implementing integrated systems. Legacy technology environments, cost constraints, organisational resistance, data-quality challenges, and limited technical expertise often impeded progress [44], [45]. The transition to integrated platforms required reconfiguration of workflows, updating of policies, redesign of control mechanisms, and retraining of staff. Furthermore, integrated systems introduced their own risks, including cybersecurity vulnerabilities, system failures, and dependency on third-party technology providers [46], [47]. Nevertheless, the potential benefits of enhanced transparency and compliance motivated many organisations particularly banks, regulatory bodies, and financial intermediaries to invest in integrated approaches [48], [49].

The social and economic significance of financial transparency underscores the importance of reviewing integrated data-compliance systems. Transparency supports financial inclusion, reduces corruption, promotes accountability in public finance, and enables equitable market participation [50]. Weak transparency can facilitate money laundering, tax evasion, fraud, and mismanagement of public resources. Integrated systems therefore serve as mechanisms for both governance reform and economic development, giving policymakers and institutions tools to strengthen the integrity of financial systems [51], [52].

Given the rising importance of data-driven oversight, this paper aims to contribute to the discourse by reviewing the state of integrated data-compliance systems up to 2017, analysing their role in enhancing transparency, and synthesising insights relevant to policymakers, regulators, institutions, and researchers. The objective is to clarify the evolution of integrated systems, their key technological and governance components, their implementation challenges, and their potential pathways for strengthening financial transparency. By structuring the review around pre-2018 developments, the paper avoids post-2017 innovations while capturing the substantial transformation that occurred during the decade leading to 2018.

This review proceeds as follows. Section 2 examines the literature on integrated data systems, compliance frameworks, RegTech developments, and transparency mechanisms prior to 2018. Section 3 synthesises theoretical and practical findings to articulate the conceptual underpinnings of integrated data-compliance ecosystems. Section 4 discusses the implications of integrated systems for governance, transparency, and financial stability. Section 5 concludes with recommendations for future research and institutional practice.

II. LITERATURE REVIEW

Financial transparency has long been recognised as a central pillar of financial stability and market integrity, but the mechanisms through which transparency is produced have evolved considerably, particularly with the emergence of integrated data systems and regulatory compliance technologies [53], [54]. Prior to 2018, financial institutions, regulatory agencies, and oversight bodies increasingly relied on digital infrastructure to strengthen transparency, improve data accuracy, and enhance real-time compliance capacity [55], [56]. The literature reveals several interconnected themes: the evolution of integrated financial information systems, the development of automated and technology-enabled compliance mechanisms, advances in regulatory data collection and reporting standards, the rise of early regulatory technology (RegTech) innovations, and challenges associated with data governance, standardisation, and cross-border regulatory harmonisation. Together, these strands form the conceptual foundation for modern transparency-oriented compliance architectures [57], [58].

2.1 Evolution of Integrated Financial Information Systems

Integrated financial information systems have their origins in early enterprise resource planning (ERP) and management information system (MIS) frameworks. These systems sought to combine financial, operational, and administrative data into a unified digital environment that allowed for more streamlined reporting and greater managerial oversight. Prior to 2018, ERP systems such as SAP, Oracle Financials, and various customised platforms provided institutions with mechanisms to integrate

accounting data, risk information, customer records, and transaction histories under common architectures [1]. The literature describes these systems as essential for eliminating data silos, reducing manual reconciliation tasks, and providing reliable audit trails. As financial institutions expanded in scale and complexity, the need for integrated architectures became more pronounced, given the proliferation of digital channels and the growing volume of transactions.

Integrated systems also played a substantial role in improving internal control environments. By providing uniform data structures and centralised repositories, such systems enabled institutions to maintain consistent financial ledgers, reduce duplication of entries, detect inconsistencies, and support continuous audit mechanisms [2]. Researchers note that the consolidation of financial data improves transparency not only for internal users, such as management and boards of directors, but also for external stakeholders, including regulators, investors, and credit-rating agencies. The quality and coherence of integrated financial information systems are directly linked to institutions' ability to produce accurate financial statements, meet regulatory deadlines, and demonstrate compliance with prudential standards.

2.2 Regulatory Reporting and Compliance Frameworks Prior to 2018

Regulatory reporting frameworks played an increasingly important role in shaping the design and evolution of integrated data systems. Over the decade preceding 2018, regulatory reforms around the world placed greater emphasis on the accuracy, timeliness, granularity, and traceability of financial data. Basel II and Basel III introduced extensive reporting requirements on capital adequacy, liquidity coverage, risk-weighted assets, and stress testing, compelling banks to adopt sophisticated data-management systems capable of consolidating risk information across business units [3]. Similarly, anti-money laundering (AML) directives and know-your-customer (KYC) guidelines required the integration of customer identity data, transactional records, and risk classification processes.

In the corporate sector, international financial reporting standards (IFRS) and similar frameworks mandated comprehensive disclosures that could only be reliably produced through integrated systems that ensured consistency across subsidiaries and departments. The literature documents an increasing move toward standardised formats for electronic data submission, such as Extensible Business Reporting Language (XBRL), which enabled regulators to process large volumes of financial information efficiently and consistently [4]. The adoption of XBRL across jurisdictions demonstrated the importance of harmonising data standards to facilitate transparency and comparability. Many financial institutions found it necessary to adapt their reporting infrastructures to support XBRL-based submissions, leading to significant investments in data architecture and compliance technologies.

Furthermore, financial crime regulations particularly those associated with AML, counter-terrorist financing (CTF), and sanctions compliance reinforced the significance of integrated compliance systems. Transaction monitoring systems, suspicious activity reporting tools, and sanctions-screening platforms increasingly relied on consolidated data inputs and automated detection logic. These systems required institutions to harmonise diverse data sources, improve data quality, and establish closed-loop compliance workflows that combined automated alerts with manual investigation procedures [5]. As non-compliance penalties escalated globally before 2018, institutions placed greater emphasis on strengthening the technological infrastructure underpinning compliance and reporting functions.

2.3 Emergence of Pre-2018 Regulatory Technology (RegTech)

Although RegTech became a prominent concept after 2018, the foundational technologies and early applications were widely documented before that time. Pre-2018 RegTech literature identifies the use of analytics, automated data feeds, unified reporting platforms, rule-based monitoring engines, and workflow tools designed to simplify compliance activities [59]. These early systems sought to reduce the cost, time, and manual burden of compliance while improving accuracy and consistency. Researchers

noted that pre-2018 RegTech was largely rule-based, relying on structured data and predetermined logic to identify compliance deviations [60], [61]. More advanced machine learning-based systems emerged only in later years, and therefore the literature prior to 2017 focuses on deterministic models rather than adaptive algorithms [62], [63], [64].

Pre-2018 RegTech also emphasised the importance of interoperability between financial databases and regulatory platforms [65], [66]. For example, integration between core banking systems, transaction monitoring engines, and AML databases became essential for achieving real-time compliance. Institutions adopting early RegTech solutions were able to automate significant portions of their reporting processes, reduce duplication, and submit standardised, regulator-ready data packages [67]. Several studies highlight that while early RegTech improved transparency, its adoption faced practical barriers such as integration difficulty, inconsistent data definitions, and insufficient alignment with existing legacy systems [68].

2.4 Data Governance and Financial Transparency

Data governance is a recurring theme in pre-2018 literature on integrated financial systems. Researchers consistently argue that transparency depends not only on the existence of integrated systems but also on the quality, accuracy, and consistency of underlying data [69]. Data governance frameworks emphasise metadata management, data stewardship, quality controls, and standardisation across enterprise datasets. Without strong data governance, integrated systems merely combine flawed or inconsistent information, which undermines transparency [70], [71].

Several studies link data governance directly to compliance effectiveness, noting that regulatory reporting failures often stem not from inadequate systems but from poor data definitions, missing values, manual override errors, and internal inconsistencies [72], [73]. Effective governance ensures that data feeding into compliance engines, reporting systems, and monitoring tools is accurate, complete, and traceable. Pre-2018 regulators increasingly stressed the need for financial institutions to formalise governance practices, including establishing data ownership roles, validating data inputs, and implementing automated quality checks. International bodies such as the Financial Stability Board (FSB) encouraged the adoption of standardised global identifiers and taxonomies to support better transparency, particularly in cross-border transactions [74], [75].

Data governance literature also highlights the challenge of reconciling data from multiple jurisdictions, each with its own regulatory definitions, formats, and reporting requirements. This fragmentation complicates both compliance processes and transparency, as institutions must reconcile local regulatory expectations with global standards. Integrated systems partially mitigate this challenge but cannot fully overcome it without harmonised policy frameworks.

2.5 Compliance Risk Management and Monitoring Systems

Prior to 2018, compliance risk management evolved from reactive, audit-driven processes to more proactive and integrated monitoring systems. Compliance monitoring literature emphasises automation, continuous controls, and exception-based reporting as mechanisms for improving transparency and preventing misconduct [76]. Integrated monitoring systems consolidate data from transactions, customer behaviour, credit operations, treasury activities, and external reporting into centralised risk dashboards that support real-time oversight [77], [78].

These systems enable institutions to detect anomalies more quickly, such as unusual transaction patterns, suspicious cross-border transfers, inconsistent accounting entries, or deviations from credit policy [79], [80]. Because transparency depends on timely detection of irregularities, automated monitoring tools significantly enhance the capacity of institutions to identify potential violations before they escalate into larger compliance breaches [81], [82]. The literature also notes that integrated monitoring improves internal audit functions, enabling auditors to examine complete datasets rather than relying on limited samples [83], [84]. This strengthens the reliability and completeness of transparency mechanisms across the entire financial reporting cycle.

Compliance monitoring literature additionally highlights the importance of workflow integration, where alerts generated by monitoring systems are fed into structured case-management tools that support investigation, documentation, and escalation procedures. Integrated workflows ensure that monitoring outputs translate into corrective actions, thereby enhancing both compliance efficiency and transparency [85], [86]. Without such integration, anomalies may be detected but not adequately addressed, weakening the transparency chain [87], [88].

2.6 Internal Controls and Transparency Enhancement

Internal control literature prior to 2018 emphasises that transparency is inseparable from effective internal control environments. Internal controls notably those associated with financial reporting, risk management, audit trails, segregation of duties, and authorization processes serve as foundational elements of transparency [89], [90]. Integrated systems enhance internal controls by reducing manual errors, creating verifiable digital records, and enabling continuous validation of financial processes [91], [92].

The literature highlights that internal control failures were frequently associated with inconsistent data sources, fragmented reporting systems, or inadequate technology infrastructure. Integrated data environments significantly reduce such vulnerabilities by enforcing consistency, automating validation checks, and improving traceability. Additionally, internal control frameworks such as COSO and COBIT emphasised the role of information systems in supporting transparency, arguing that technology-enabled controls are more reliable and scalable than manual processes [93], [94].

Scholars observed that institutions with integrated data and strong internal control systems were better equipped to withstand external shocks, mitigate fraud risk, and satisfy the reporting expectations of regulators. Conversely, organisations with fragmented systems often struggled to ensure transparency during crisis periods, when the need for accurate and timely information becomes most urgent.

2.7 Cross-Border Regulation and International Transparency Initiatives

Financial markets are global, and therefore transparency challenges often extend across multiple jurisdictions. Pre-2018 literature discusses the difficulties of standardising reporting, harmonising compliance obligations, and coordinating supervisory efforts internationally [95], [96]. Cross-border regulation requires consistent definitions of financial products, risk categories, and reporting timelines. Integrated systems that support harmonised taxonomies help improve transparency by reducing discrepancies between jurisdictions and enabling consolidated reporting.

International initiatives such as the Financial Action Task Force (FATF) AML standards, the Common Reporting Standard (CRS) for tax transparency, and global trade repository requirements for derivatives transactions demonstrate the growing emphasis on international transparency. These initiatives required institutions to develop systems capable of standardising data inputs, aggregating global account information, and communicating with international regulatory platforms [97], [98]. The literature identifies several implementation challenges, including inconsistent data standards, limited interoperability of national systems, and inconsistent regulatory interpretation. Nevertheless, early cross-border transparency frameworks laid the groundwork for more robust international supervisory cooperation.

2.8 Challenges in Implementing Integrated Data and Compliance Systems

Despite advancements, several obstacles both technical and organisational hindered the full implementation of integrated systems prior to 2018. Legacy systems posed one of the greatest barriers, as many institutions relied on outdated platforms that lacked flexibility, produced incompatible data formats, or could not support real-time reporting. Integrating new compliance technologies with these legacy systems required significant financial investment, architectural redesign, and specialist expertise [99].

Data quality challenges also persisted, including incomplete records, inconsistent coding schemes,

duplicated entries, and lack of standardised identifiers [100]. These issues undermined the effectiveness of integration, as flawed data produces flawed compliance outputs [101], [102]. Organisational resistance further complicated implementation: employees accustomed to manual processes often resisted automation due to perceived job displacement, lack of familiarity with digital tools, or mistrust of system outputs [103].

Additionally, cybersecurity risks increased as institutions adopted more integrated and interconnected systems [104]. Integrated platforms offer attackers larger potential attack surfaces, requiring robust cybersecurity frameworks to prevent breaches that could compromise compliance data and financial transparency [105]. The literature emphasises that transparency and security must be parallel objectives in any integrated system design [106].

2.9 Synthesis of Literature and Conceptual Foundations

A synthesis of the pre-2018 literature demonstrates that integrated data and compliance systems significantly enhance financial transparency by improving data quality, increasing automation, enabling real-time monitoring, and supporting regulatory reporting. The literature shows strong convergence across domains accounting, compliance, data governance, financial regulation, and information systems regarding the central role of integration in promoting transparency.

Researchers consistently link integration to improved internal controls, more accurate risk assessment, greater organisational accountability, and enhanced regulatory compliance. RegTech developments, though relatively nascent prior to 2018, further contributed to the evolution of compliance systems by demonstrating the benefits of automation, interoperability, and digital reporting workflows. At the same time, practical barriers such as legacy-system constraints, data-quality shortcomings, and cross-border regulatory fragmentation persisted as significant limitations.

Overall, the literature up to 2017 provides a strong theoretical foundation for understanding the potential of integrated data and compliance systems to strengthen financial transparency. It also highlights the need for continued innovation within pre-2018 capabilities combined with organisational reform and robust data governance practices.

III. DISCUSSION

The review of pre-2018 literature reveals that integrated data and compliance systems play a transformative role in strengthening financial transparency by aligning technological capabilities, regulatory expectations, and institutional governance practices. This section synthesises the central insights from the preceding review and examines how integrated systems influence transparency at organisational, regulatory, and systemic levels. It also considers the practical implications, structural constraints, and strategic challenges associated with implementing such systems. The discussion highlights the ways in which integrated data-compliance ecosystems advance transparency beyond what traditional reporting and manual compliance processes can achieve, while acknowledging the limitations that must be managed for these systems to function effectively.

A primary reflection emerging from the literature is that financial transparency depends heavily on the quality, coherence, and accessibility of financial data. Integrated systems significantly enhance these characteristics by unifying previously fragmented data sources, establishing consistent definitions, and enforcing standardised financial taxonomies across organisations. When financial data reside in silos, inconsistencies inevitably arise in accounting records, regulatory reports, risk assessments, and internal audits. Such fragmentation obstructs transparency by creating opportunities for misrepresentation, masking emerging risks, or generating reporting errors. Integrated systems solve this by providing a common data architecture that connects core banking systems, transaction databases, risk platforms, and compliance tools into a unified environment. This integration improves the auditability of financial information, supports real-time oversight, and enhances the accuracy of regulatory submissions all essential elements of transparency.

Another major theme is the relationship between regulatory reform and the adoption of integrated systems. Prior to 2018, regulatory bodies increasingly demanded detailed, frequent, and verifiable data from financial institutions. These expectations were shaped by reforms such as Basel III, AML/KYC directives, IFRS requirements, and global initiatives on tax transparency and systemic risk reporting. The literature shows that regulatory pressure served as a powerful catalyst for the adoption of integrated data-compliance technologies. Institutions were compelled to invest in systems capable of supporting extensive reporting obligations, managing structured regulatory data formats, and maintaining accurate records across departments. As regulatory complexity increased, manual compliance mechanisms became inadequate, forcing institutions to adopt automated data pipelines, integrated reporting engines, and structured digital submission formats such as XBRL. The interaction between regulatory complexity and technological capability thus produced a mutually reinforcing cycle: stronger regulations encouraged system integration, while better integrated systems improved compliance efficiency and transparency.

The discussion also highlights the emergence of early RegTech solutions as an important innovation within pre-2018 transparency efforts. Although far less advanced than the machine-learning-driven systems that emerged after 2018, early RegTech played a foundational role in automating compliance tasks, including transaction monitoring, rule-based exception reporting, identity verification, and data validation. These systems demonstrated that compliance workflows could transition from reactive, audit-driven processes to more continuous, proactive forms of oversight. The capacity to detect anomalies in near real time for example, unusual transaction patterns, sanctions violations, or regulatory breaches marked a significant enhancement in transparency. Institutions with integrated monitoring systems were able to identify and respond to suspicious activities or reporting discrepancies far more efficiently than those using traditional manual controls. The literature suggests that these early technologies pointed to a future in which compliance is embedded directly into operational processes, reinforcing transparency through continual system-driven checks rather than periodic reviews.

The role of data governance emerges as another important dimension affecting transparency. Integrated systems cannot achieve their intended goals if the underlying data are inaccurate, incomplete, or inconsistently defined. The literature demonstrates that data governance challenges such as inconsistent metadata, duplicated customer information, non-standardised financial codes, and legacy-system incompatibilities were among the most persistent barriers to transparency before 2018. Effective transparency therefore requires a parallel investment in governance practices that ensure data accuracy and traceability. Institutions with mature data governance frameworks were significantly more capable of using integrated systems to strengthen transparency, whereas those lacking governance discipline struggled to produce reliable compliance outputs despite having advanced systems. This finding underscores that technology alone cannot solve transparency issues; institutional culture, governance maturity, and organisational discipline play decisive roles in determining outcomes.

Integrated systems also influence transparency by reshaping the internal control environment. Strong internal controls are essential for producing trustworthy financial information, and integrated systems reinforce these controls by automating validation processes, establishing digital audit trails, and reducing reliance on manual intervention. The literature highlights that internal control failures such as improperly reconciled accounts, unverified transactions, or weak segregation of duties are key contributors to transparency breakdowns. Integrated systems mitigate these failures by embedding controls directly into transaction flows, enabling continuous verification, and supporting end-to-end supervision across the financial reporting cycle. These capabilities are particularly relevant to financial institutions operating across multiple jurisdictions, where internal control processes must accommodate different regulatory expectations and reporting templates. Integration ensures that internal controls operate consistently regardless of geographic or organisational boundaries, thereby strengthening both transparency and compliance reliability.

Cross-border financial activities present another important context where integrated systems

significantly enhance transparency. International financial flows often involve multiple regulatory regimes, each with its own reporting requirements, legal definitions, and compliance frameworks. Without integrated systems, financial institutions struggle to reconcile data across jurisdictions, leading to reporting inconsistencies and delays that undermine transparency. Pre-2018 international transparency initiatives such as FATF standards, CRS tax reporting, and global derivative trade repositories relied heavily on data harmonisation and consistent compliance processes across institutions and countries. Integrated systems help meet these requirements by standardising global account information, harmonising data structures, and enabling consolidated reporting. Through such mechanisms, integration supports international supervisory cooperation and reduces opportunities for regulatory arbitrage, tax evasion, and cross-border money-laundering activities.

Despite these benefits, the discussion must also acknowledge the challenges associated with implementing integrated systems, which are thoroughly documented in the literature. Legacy technology remains one of the most significant obstacles. Many institutions prior to 2018 relied on decades-old infrastructure that lacked interoperability, depended on outdated coding languages, or operated through siloed system architectures. The cost, complexity, and operational risk of replacing or modernising such systems were substantial, limiting the ability of institutions particularly smaller or resource-constrained ones to adopt advanced integration. Another major challenge relates to organisational resistance. Employees accustomed to manual procedures often resisted automation due to concerns about job impacts, lack of trust in digital tools, or limited digital literacy. Such resistance created organisational friction that slowed the adoption of integrated systems and undermined transparency objectives.

Cybersecurity risks also intensified as institutions adopted more integrated and interconnected technologies. Integrated systems consolidate sensitive financial data, making them attractive targets for cyberattacks. A breach in an integrated environment can result in large-scale exposure of financial records, customer information, and compliance data. The literature emphasises that cybersecurity and transparency must be treated as interdependent goals: transparency requires integrated data to be accessible and reliable, while cybersecurity demands that access be controlled and protected from malicious activity. Institutions must therefore balance openness with security, implementing strong access controls, encryption standards, intrusion detection systems, and operational resilience frameworks.

A further concern identified in the literature relates to the uneven regulatory harmonisation across jurisdictions. Integrated systems can only achieve full transparency when data standards, regulatory definitions, and compliance expectations are aligned across agencies and countries. Without such harmonisation, institutions face costly and complex requirements to develop multiple reporting templates, reconcile conflicting definitions, and maintain parallel compliance systems. Integrated platforms partially address these inconsistencies by providing consolidated data structures, but they cannot eliminate differences in regulatory interpretation or jurisdictional demands. This tension between global integration and local regulation is a recurring theme in discussions on the limits of transparency prior to 2018.

In broader conceptual terms, the discussion demonstrates that integrated data and compliance systems are more than technological tools they represent a shift in how transparency is conceptualised and operationalised within financial systems. Transparency is no longer merely a function of periodic reporting; rather, it becomes a continuous, dynamic process supported by data pipelines, automated controls, real-time monitoring, and coordinated governance structures. Integrated systems treat transparency as an ongoing organisational state rather than a quarterly or annual output. This transformation has significant implications for internal audit, compliance officers, risk managers, and regulators, whose roles increasingly involve interpreting system outputs, monitoring data flows, and managing digital compliance ecosystems.

Overall, the literature suggests that integrated data and compliance systems significantly enhance financial transparency by bridging gaps between regulation, technology, and institutional governance. However,

their effectiveness depends on factors such as data governance maturity, organisational readiness, regulatory clarity, and system security. Integrated systems thus offer a powerful pathway toward transparency, but they must be supported by strong governance, standardisation efforts, and coordinated implementation strategies to address persistent challenges. The discussion sets the stage for concluding reflections on how these insights can inform future research and guide institutions seeking to strengthen transparency within the constraints of pre-2018 technological and regulatory contexts.

IV. CONCLUSION

The review of integrated data and compliance systems up to 2017 demonstrates that financial transparency is fundamentally shaped by the degree of technological integration, regulatory alignment, and organisational governance embedded within financial institutions. As markets evolved and regulatory requirements intensified in the years prior to 2018, institutions increasingly recognised that traditional manual and fragmented compliance processes were inadequate for addressing the complexity, scale, and velocity of modern financial activity. Integrated systems emerged as a necessary response to these challenges, enabling institutions to consolidate data from diverse operational channels, automate compliance workflows, and strengthen the reliability, accuracy, and timeliness of financial reporting. These systems not only addressed regulatory expectations but also supported broader goals related to institutional accountability, risk management, and public trust.

The literature consistently affirms that transparency cannot be achieved through technology alone; rather, it requires an integrated ecosystem where data governance, organisational culture, internal controls, and compliance processes function in coordination. Institutions with robust data governance frameworks defined by standardised definitions, consistent taxonomies, and clear ownership structures demonstrated greater capability to leverage integrated systems effectively. Conversely, institutions lacking disciplined governance struggled to realise transparency gains even when advanced systems were deployed. This distinction reinforces the understanding that integration must be accompanied by organisational reforms that prioritise data quality, traceability, and accountability.

Integrated systems also provided significant enhancements to compliance monitoring and regulatory reporting, areas where transparency is most frequently scrutinised. Automated compliance engines, early RegTech applications, and consolidated reporting frameworks reduced the likelihood of reporting errors, improved the speed of regulatory submissions, and supported more rigorous oversight. By embedding compliance logic within operational processes, financial institutions shifted from periodic, reactive compliance assessments to more proactive, continuous monitoring. This shift improved the capacity to detect anomalies, prevent financial misconduct, and ensure that financial information reflected real-time organisational realities. Such capabilities are particularly important in globalised financial environments where cross-border transactions, complex group structures, and jurisdictional variations in regulation create additional transparency challenges.

Despite these significant advancements, the review highlights important limitations that continued to hinder transparency efforts prior to 2018. Legacy systems remained a major obstacle, often lacking interoperability or requiring costly and complex integration work. Data quality issues, including inconsistent coding, missing values, and duplicated entries, frequently undermined the integrity of integrated systems. Organisational resistance also slowed adoption, as employees accustomed to manual processes resisted digital transformation. Moreover, cybersecurity concerns, exacerbated by increasingly interconnected systems, introduced new risks that institutions had to manage to preserve the confidentiality and integrity of compliance-critical data. These limitations demonstrate that integration is not a one-time technical exercise but an ongoing strategic effort requiring sustained investment and governance commitment.

International regulatory fragmentation further constrained the full potential of integrated systems. While integrated platforms could harmonise internal data structures, they could not resolve divergent regulatory requirements across jurisdictions. The

resulting need for multiple reporting formats and reconciliation processes placed continued pressure on compliance functions. Nevertheless, early cross-border initiatives—such as AML standards, tax-transparency frameworks, and global securities reporting—improved the landscape by establishing shared expectations and promoting convergence, even if inconsistencies persisted.

Looking across the pre-2018 period, the evidence suggests that integrated data and compliance systems represent a foundational step toward increasingly transparent and accountable financial systems. They address fundamental weaknesses in legacy reporting structures, improve the reliability of financial disclosures, enhance supervisory oversight, and support more resilient internal control environments. While challenges remain, integrated systems create the structural conditions needed for financial transparency to evolve from periodic reporting into a continuous organisational capability.

Future research may build on these pre-2018 foundations by exploring how institutions can strengthen data governance maturity, develop interoperable regulatory frameworks, improve system security, and expand the role of automation in compliance processes. Institutional practice must similarly evolve, requiring sustained investment in integration, training, cybersecurity, and regulatory harmonisation. Although transparency is shaped by technological capacity, it ultimately depends on organisational commitment to accuracy, accountability, and ethical conduct—principles that remain essential regardless of technological advances.

In conclusion, integrated data and compliance systems significantly advance financial transparency by unifying information flows, enhancing reporting integrity, supporting continuous oversight, and strengthening the capacity of institutions to meet regulatory expectations. As financial systems continue to grow in complexity, these integrated architectures provide a critical foundation for building transparent, resilient, and trustworthy financial institutions capable of supporting sustainable economic development and maintaining public confidence in financial markets.

REFERENCES

[1] W. K. T. Cho and B. J. Gaines, “Breaking the (Benford) law: Statistical fraud detection in campaign finance,” *American Statistician*, vol. 61, no. 3, pp. 218–223, Aug. 2007, doi: 10.1198/000313007X223496.

[2] I. Hasan, K. Jackowicz, O. Kowalewski, and Ł. Kozłowski, “Do local banking market structures matter for SME financing and performance? New evidence from an emerging economy,” *J Bank Financ*, vol. 79, pp. 142–158, Jun. 2017, doi: 10.1016/J.JBANKFIN.2017.03.009.

[3] M. Sipa, I. Gorzeń-Mitka, and A. Skibiński, “Determinants of Competitiveness of Small Enterprises: Polish Perspective,” *Procedia Economics and Finance*, vol. 27, pp. 445–453, 2015, doi: 10.1016/S2212-5671(15)01019-9.

[4] N. E. Popescu, “Entrepreneurship and SMEs Innovation in Romania,” *Procedia Economics and Finance*, vol. 16, pp. 512–520, 2014, doi: 10.1016/S2212-5671(14)00832-6.

[5] M. D. Gould, M. A. Porter, S. Williams, M. McDonald, D. J. Fenn, and S. D. Howison, “Limit order books,” *Quant Finance*, vol. 13, no. 11, pp. 1709–1742, 2013, doi: 10.1080/14697688.2013.803148.

[6] S. Mullainathan, J. Schwartzstein, and W. J. Congdon, “A reduced-form approach to behavioral public finance,” *Annu Rev Econom*, vol. 4, pp. 511–540, Jul. 2012, doi: 10.1146/ANNUREV-ECONOMICS-111809-125033.

[7] P. C. Tetlock, “Information transmission in finance,” *Annual Review of Financial Economics*, vol. 6, pp. 365–384, Dec. 2014, doi: 10.1146/ANNUREV-FINANCIAL-110613-034449.

[8] D. Hirshleifer, “Behavioral Finance,” *Annual Review of Financial Economics*, vol. 7, no. Volume 7, 2015, pp. 133–159, Dec. 2015, doi: 10.1146/ANNUREV-FINANCIAL-092214-043752/CITE/REFWORKS.

[9] P. M. Hartmann, M. Zaki, N. Feldmann, and A. Neely, "Capturing value from big data–a taxonomy of data-driven business models used by start-up firms," *International Journal of Operations & Production Management*, vol. 36, no. 10, pp. 1382–1406, 2016, doi: 10.1108/ijopm-02-2014-0098.

[10] S. Barocas and H. Nissenbaum, "Big data's end run around procedural privacy protections," *Commun ACM*, vol. 57, no. 11, pp. 31–33, Nov. 2014, doi: 10.1145/2668897.

[11] J. W. Y Zhang, "Data-driven modeling and scientific computing," *Appl Mech Rev*, vol. 68, no. 5, pp. 050801–051013, 2016.

[12] P. Li *et al.*, "Promoting secondary analysis of electronic medical records in china: Summary of the plagh-mit critical data conference and health datathon," *JMIR Med Inform*, vol. 5, no. 4, Oct. 2017, doi: 10.2196/MEDINFORM.7380.

[13] J. Hemerly, "Public policy considerations for data-driven innovation," *Computer (Long Beach Calif)*, vol. 46, no. 6, pp. 25–31, 2013, doi: 10.1109/MC.2013.186.

[14] S. Fosso Wamba, S. Akter, A. Edwards, G. Chopin, and D. Gnanzou, "How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study," *Int J Prod Econ*, vol. 165, pp. 234–246, Jul. 2015, doi: 10.1016/J.IJPE.2014.12.031.

[15] P. Kadlec, B. Gabrys, and S. Strandt, "Data-driven Soft Sensors in the process industry," *Comput Chem Eng*, vol. 33, no. 4, pp. 795–814, Apr. 2009, doi: 10.1016/j.compchemeng.2008.12.012.

[16] M. A. Waller and S. E. Fawcett, "Data science, predictive analytics, and big data: A revolution that will transform supply chain design and management," *Journal of Business Logistics*, vol. 34, no. 2, pp. 77–84, 2013, doi: 10.1111/JBL.12010.

[17] A. Geissbuhler *et al.*, "Trustworthy reuse of health data: A transnational perspective," *Int J Med Inform*, vol. 82, no. 1, pp. 1–9, Jan. 2013, doi: 10.1016/J.IJMEDINF.2012.11.003.

[18] J. A. Burkell, "Remembering me: big data, individual identity, and the psychological necessity of forgetting," *Ethics Inf Technol*, vol. 18, no. 1, pp. 17–23, Mar. 2016, doi: 10.1007/S10676-016-9393-1.

[19] C. Meng, S. S. Nageshwaraniyer, A. Maghsoudi, Y. J. Son, and S. Dessureault, "Data-driven modeling and simulation framework for material handling systems in coal mines," *Comput Ind Eng*, vol. 64, no. 3, pp. 766–779, 2013, doi: 10.1016/J.CIE.2012.12.017.

[20] J. Sandefur and A. Glassman, "The Political Economy of Bad Data: Evidence from African Survey and Administrative Statistics," *Journal of Development Studies*, vol. 51, no. 2, pp. 116–132, Feb. 2015, doi: 10.1080/00220388.2014.968138.

[21] K. Witkowski, "Internet of Things, Big Data, Industry 4.0 - Innovative Solutions in Logistics and Supply Chains Management," *Procedia Eng*, vol. 182, pp. 763–769, 2017, doi: 10.1016/j.proeng.2017.03.197.

[22] A. Kaushik and A. Raman, "The new data-driven enterprise architecture for e-healthcare: Lessons from the indian public sector," *Gov Inf Q*, vol. 32, no. 1, pp. 63–74, 2015, doi: 10.1016/J.GIQ.2014.11.002.

[23] D. Li, W. Daamen, and R. M. P. Goverde, "Estimation of train dwell time at short stops based on track occupation event data: A study at a Dutch railway station," *J Adv Transp*, vol. 50, no. 5, pp. 877–896, Aug. 2016, doi: 10.1002/ATR.1380.

[24] S. Rosenbaum, "Data governance and stewardship: Designing data stewardship entities and advancing data access," *Health Serv Res*, vol. 45, no. 5 PART 2, pp. 1442–1455, Oct. 2010, doi: 10.1111/J.1475-6773.2010.01140.X.

[25] V. Khatri and C. V. Brown, "Designing data governance," *Commun ACM*, vol. 53, no. 1, pp. 148–152, Jan. 2010, doi: 10.1145/1629175.1629210.

[26] S. O'Riain, E. Curry, and A. Harth, "XBRL and open data for global financial ecosystems: A linked data approach," *International Journal of Accounting Information Systems*, vol. 13, no. 2, pp. 141–162, Jun. 2012, doi: 10.1016/J.ACCINF.2012.02.002.

[27] A. Halevy, P. Norvig, and F. Pereira, "The unreasonable effectiveness of data," *IEEE Intell Syst*, vol. 24, no. 2, pp. 8–12, 2009, doi: 10.1109/MIS.2009.36.

[28] J. Fan, F. Han, and H. Liu, "Challenges of Big Data analysis," *Natl Sci Rev*, vol. 1, no. 2, pp. 293–314, Jun. 2014, doi: 10.1093/NSR/NWT032.

[29] L. Edwards, "Privacy, Security and Data Protection in Smart Cities:," *European Data Protection Law Review*, vol. 2, no. 1, pp. 28–58, Feb. 2017, doi: 10.21552/EDPL/2016/1/6.

[30] C. Allen *et al.*, "Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities," *EGEMS*, vol. 2, no. 1, p. 1057, Apr. 2014, doi: 10.13063/2327-9214.1057.

[31] L. Cheng, F. Liu, and D. D. Yao, "Enterprise data breach: causes, challenges, prevention, and future directions," *Wiley Interdiscip Rev Data Min Knowl Discov*, vol. 7, no. 5, Sep. 2017, doi: 10.1002/WIDM.1211.

[32] F. H. Cate and V. Mayer-Schönberger, "Tomorrow's privacy: Notice and consent in a world of Big Data," *International Data Privacy Law*, vol. 3, no. 2, pp. 67–73, May 2013, doi: 10.1093/IDPL/IPT005.

[33] R. Schroeder, "Big Data and the brave new world of social media research," *Big Data Soc*, vol. 1, no. 2, Jul. 2014, doi: 10.1177/2053951714563194.

[34] A. O'Cathain, E. Murphy, and J. Nicholl, "Three techniques for integrating data in mixed methods studies," *BMJ*, vol. 341, no. 7783, pp. 1147–1150, Nov. 2010, doi: 10.1136/bmj.c4587.

[35] W. Wang, M. Winner, and C. R. Burgert-Brucker, "Limited service availability, readiness, and use of facility-based delivery care in Haiti: A study linking health facility data and population data," *Glob Health Sci Pract*, vol. 5, no. 2, pp. 244–261, Jun. 2017, doi: 10.9745/GHSP-D-16-00311.

[36] E. Baccarelli, N. Cordeschi, A. Mei, M. Panella, M. Shojafar, and J. Stefa, "Energy-efficient dynamic traffic offloading and reconfiguration of networked data centers for big data stream mobile computing: Review, challenges, and a case study," *IEEE Netw*, 2016.

[37] N. Terry, "Existential challenges for healthcare data protection in the United States," *Ethics Med Public Health*, vol. 3, no. 1, pp. 19–27, Jan. 2017, doi: 10.1016/J.JEMEP.2017.02.007.

[38] L. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, "Cloud Computing Model and Big Data Analysis for Healthcare Applications," *IEEE Access*, vol. 4, 2016.

[39] B. Baesens, R. Bapna, J. R. Marsden, J. Vanthienen, and J. L. Zhao, "Transformational issues of big data and analytics in networked business," *MIS Quarterly*, vol. 40, no. 4, pp. 807–818, Dec. 2016, doi: 10.25300/misq/2016/40:4.03.

[40] Y. Sun and S. Upadhyaya, "Secure and privacy preserving data processing support for active authentication," *Information Systems Frontiers*, vol. 17, no. 5, pp. 1007–1015, Oct. 2015, doi: 10.1007/s10796-015-9587-9.

[41] H. Chen, R. H. L. Chiang, and V. C. Storey, "Business intelligence and analytics: From big data to big impact," *MIS Q*, vol. 36, no. 4, pp. 1165–1188, 2012, doi: 10.2307/41703503.

[42] X. Liu, P. V. Singh, and K. Srinivasan, "A structured analysis of unstructured big data by leveraging cloud computing," *Marketing Science*, vol. 35, no. 3, pp. 363–388, May 2016, doi: 10.1287/MKSC.2015.0972.

[43] A. Gunasekaran *et al.*, "Big data and predictive analytics for supply chain and organizational performance," *J Bus Res*, vol. 70, pp. 308–317, Jan. 2017, doi: 10.1016/j.jbusres.2016.08.004.

[44] C. S. Kruse, R. Goswamy, Y. Raval, and S. Marawi, "Challenges and opportunities of big data in health care: A systematic review," *JMIR Med Inform*, vol. 4, no. 4, Oct. 2016, doi: 10.2196/MEDINFORM.5359.

[45] W. Wang and E. Krishnan, "Big data and clinicians: A review on the state of the science," *JMIR Med Inform*, vol. 2, no. 1, Jan. 2014, doi: 10.2196/MEDINFORM.2913.

[46] J. Wang, Y. Zhou, Y. Wang, J. Zhang, C. L. P. Chen, and Z. Zheng, "Multiobjective Vehicle Routing Problems with Simultaneous Delivery and Pickup and Time Windows: Formulation, Instances, and Algorithms," *IEEE Trans Cybern*, vol. 46, no. 3, pp. 582–594, Mar. 2016, doi: 10.1109/TCYB.2015.2409837.

[47] L. Oneto *et al.*, "Dynamic delay predictions for large-scale railway networks: Deep and shallow extreme learning machines tuned via thresholdout," *IEEE Trans Syst Man Cybern Syst*, vol. 47, no. 10, pp. 2754–2767, Oct. 2017, doi: 10.1109/TSMC.2017.2693209.

[48] A. V. Palagin, "Functionally oriented approach in research-related design," *Cybern. Syst. Analysis*, vol. 53, no. 6, pp. 986–992, Nov. 2017, doi: 10.1007/s10559-017-0001-0.

[49] I. G. Kryvonos, I. V. Krak, O. V. Barmak, and A. I. Kulias, "Methods to Create Systems for the Analysis and Synthesis of Communicative Information," *Cybern Syst Anal*, vol. 53, no. 6, pp. 847–856, Nov. 2017, doi: 10.1007/S10559-017-9986-7.

[50] A. Fronzetti Colladon and E. Remondi, "Using social network analysis to prevent money laundering," *Expert Syst Appl*, vol. 67, pp. 49–58, Jan. 2017, doi: 10.1016/J.ESWA.2016.09.029.

[51] L. C. Dreyer, M. Z. Hauschild, and J. Schierbeck, "A framework for social life cycle impact assessment," *International Journal of Life Cycle Assessment*, vol. 11, no. 2, pp. 88–97, Mar. 2006, doi: 10.1065/LCA2005.08.223.

[52] V. Mani, R. Agrawal, and V. Sharma, "Supplier selection using social sustainability: AHP based approach in India," *International Strategic Management Review*, vol. 2, no. 2, pp. 98–112, Dec. 2014, doi: 10.1016/j.ism.2014.10.003.

[53] N. Barberis and R. Thaler, "Chapter 18 A survey of behavioral finance," *Handbook of the Economics of Finance*, vol. 1, no. SUPPL. PART B, pp. 1053–1128, 2003, doi: 10.1016/S1574-0102(03)01027-6.

[54] R. Kersten, J. Harms, K. Liket, and K. Maas, "Small Firms, large Impact? A systematic review of the SME Finance Literature," *World Dev*, vol. 97, pp. 330–348, Sep. 2017, doi: 10.1016/J.WORLDDEV.2017.04.012.

[55] D. E. O'Leary, "Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems," *Intelligent Systems in Accounting, Finance and Management*, vol. 24, no. 4, pp. 138–147, Oct. 2017, doi: 10.1002/ISAF.1417.

[56] W. R. Kerr and R. Nanda, "Financing Innovation," *Annual Review of Financial Economics*, vol. 7, pp. 445–462, Dec. 2015, doi: 10.1146/ANNUREV-FINANCIAL-111914-041825.

[57] I. H. Cheng and W. Xiong, "Financialization of commodity markets," *Annual Review of Financial Economics*, vol. 6, pp. 419–941, Dec. 2014, doi: 10.1146/ANNUREV-FINANCIAL-110613-034432.

[58] P. Bond, A. Edmans, and I. Goldstein, "The real effects of financial markets," *Annual*

Review of Financial Economics, vol. 4, pp. 339–360, Oct. 2012, doi: 10.1146/ANNUREV-FINANCIAL-110311-101826.

[59] B. Trap *et al.*, "First regulatory inspections measuring adherence to good pharmacy practices in the public sector in uganda: A cross-sectional comparison of performance between supervised and unsupervised facilities," *J Pharm Policy Pract*, vol. 9, no. 1, pp. 1–10, 2016, doi: 10.1186/S40545-016-0068-4.

[60] L. Urquhart and T. Rodden, "New directions in information technology law: learning from human–computer interaction," *International Review of Law, Computers and Technology*, vol. 31, no. 2, pp. 150–169, May 2017, doi: 10.1080/13600869.2017.1298501.

[61] B. Boyce, "Emerging Technology and the Health Insurance Portability and Accountability Act," *J Acad Nutr Diet*, vol. 117, no. 4, pp. 517–518, Apr. 2017, doi: 10.1016/j.jand.2016.05.013.

[62] J. Abelson *et al.*, "PUBLIC and PATIENT INVOLVEMENT in HEALTH TECHNOLOGY ASSESSMENT: A FRAMEWORK for ACTION," *Int J Technol Assess Health Care*, vol. 32, no. 4, pp. 256–264, 2016, doi: 10.1017/S0266462316000362.

[63] S. Dünnebeil, A. Sunyaev, I. Blohm, J. M. Leimeister, and H. Krcmar, "Determinants of physicians' technology acceptance for e-health in ambulatory care," *Int J Med Inform*, vol. 81, no. 11, pp. 746–760, Nov. 2012, doi: 10.1016/j.ijmedinf.2012.02.002.

[64] L. M. Mutuku, "The Effect of Technology on Supply Delivery of Online Stores in Kenya," 2017, Accessed: Jul. 06, 2016. [Online]. Available: http://erepository.uonbi.ac.ke/handle/11295/102873

[65] I. Holeman, T. P. Cookson, and C. Pagliari, "Digital technology for health sector governance in low and middle income countries: A scoping review," *J Glob Health*, vol. 6, no. 2, 2016, doi: 10.7189/JOGH.06.020408.

[66] B. Chaudhry, J. Wang, S. Wu, M. Maglione, W. Mojica, and E. Roth, "Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care," *Ann Intern Med*, vol. 144, no. 10, 2006.

[67] B. Oztaysi, S. Cevik Onar, C. Kahraman, and M. Yavuz, "Multi-criteria alternative-fuel technology selection using interval-valued intuitionistic fuzzy sets," *Transp Res D Transp Environ*, vol. 53, pp. 128–148, Jun. 2017, doi: 10.1016/j.trd.2017.04.003.

[68] F. Magrabi, S. T. Liaw, D. Arachi, W. Runciman, E. Coiera, and M. R. Kidd, "Identifying patient safety problems associated with information technology in general practice: An analysis of incident reports," *BMJ Qual Saf*, vol. 25, no. 11, pp. 870–880, Nov. 2016, doi: 10.1136/BMJQS-2015-004323.

[69] D. Donoho, "50 Years of Data Science," *Journal of Computational and Graphical Statistics*, vol. 26, no. 4, pp. 745–766, Oct. 2017, doi: 10.1080/10618600.2017.1384734.

[70] A. Cerioli and D. Perrotta, "Robust clustering around regression lines with high density regions," *Adv Data Anal Classif*, vol. 8, no. 1, pp. 5–26, 2014, doi: 10.1007/S11634-013-0151-5.

[71] R. J. Hyndman, R. A. Ahmed, G. Athanasopoulos, and H. L. Shang, "Optimal combination forecasts for hierarchical time series," *Comput Stat Data Anal*, vol. 55, no. 9, pp. 2579–2589, Sep. 2011, doi: 10.1016/J.CSDA.2011.03.006.

[72] H. Demirkan and D. Delen, "Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud," *Decis Support Syst*, vol. 55, no. 1, pp. 412–421, Apr. 2013, doi: 10.1016/j.dss.2012.05.048.

[73] J. H. Hibbard and E. Peters, "Supporting informed consumer health care decisions: data presentation approaches that facilitate the use of information in choice," *Annu Rev Public Health*, vol. 24, pp. 413–33, 2003, doi: 10.1146/annurev.publhealth.24.100901.141005.

[74] J. Wang and H. Yue, "Food safety pre-warning system based on data mining for a sustainable food supply chain," *Food Control*, vol. 73, pp. 223–229, Mar. 2017, doi: 10.1016/J.FOODCONT.2016.09.048.

[75] R. Ramanathan, U. Ramanathan, and Y. Zhang, "Linking operations, marketing and environmental capabilities and diversification to hotel performance: A data envelopment analysis approach," *Int J Prod Econ*, vol. 176, pp. 111–122, Jun. 2016, doi: 10.1016/j.ijpe.2016.03.010.

[76] J. P. Belaud, S. Negny, F. Dupros, D. Michéa, and B. Vautrin, "Collaborative simulation and scientific big data analysis: Illustration for sustainability in natural hazards management and chemical process engineering," *Comput Ind*, vol. 65, no. 3, pp. 521–535, 2014, doi: 10.1016/j.compind.2014.01.009.

[77] G. Sarens, I. De Beelde, and P. Everaert, "Internal audit: A comfort provider to the audit committee," *British Accounting Review*, vol. 41, no. 2, pp. 90–106, Jun. 2009, doi: 10.1016/J.BAR.2009.02.002.

[78] K. A. Endaya and M. M. Hanefah, "Internal auditor characteristics, internal audit effectiveness, and moderating effect of senior management," *Journal of Economic and Administrative Sciences*, vol. 32, no. 2, pp. 160–176, 2016, doi: 10.1108/JEAS-07-2015-0023.

[79] G. Sarens and I. De Beelde, "Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies," *Managerial Auditing Journal*, vol. 21, no. 1, pp. 63–80, 2006, doi: 10.1108/02686900610634766.

[80] L. de Zwaan, J. Stewart, and N. Subramaniam, "Internal audit involvement in enterprise risk management," *Managerial Auditing Journal*, vol. 26, no. 7, pp. 586–604, Jul. 2011, doi: 10.1108/02686901111151323.

[81] R. Lenz, G. Sarens, and F. Hoos, "Internal Audit Effectiveness: Multiple Case Study Research Involving Chief Audit Executives and Senior Management," *EDPACS*, vol. 55, no. 1, pp. 1–17, Jan. 2017, doi: 10.1080/07366981.2017.1278980.

[82] M. Arena and G. Azzone, "Identifying Organizational Drivers of Internal Audit Effectiveness," *International Journal of Auditing*, vol. 13, no. 1, pp. 43–60, Mar. 2009, doi: 10.1111/J.1099-1123.2008.00392.X.

[83] J. Goodwin, "A comparison of internal audit in the private and public sectors," *Managerial Auditing Journal*, vol. 19, no. 5, pp. 640–650, Jun. 2004, doi: 10.1108/02686900410537766.

[84] A. Fernández-Laviada, "Internal audit function role in operational risk management," *Journal of Financial Regulation and Compliance*, vol. 15, no. 2, pp. 143–155, 2007, doi: 10.1108/13581980710744039.

[85] P. Coetzee and D. Lubbe, "Improving the efficiency and effectiveness of risk-based internal audit engagements," *International Journal of Auditing*, vol. 18, no. 2, pp. 115–125, 2014, doi: 10.1111/IJAU.12016.

[86] N. H. Z. Abidin, "Factors influencing the implementation of risk-based auditing," *Asian Review of Accounting*, vol. 25, no. 3, pp. 361–375, 2017, doi: 10.1108/ARA-10-2016-0118.

[87] K. Govindan and H. Soleimani, "A review of reverse logistics and closed-loop supply chains: a Journal of Cleaner Production focus," *J Clean Prod*, vol. 142, pp. 371–384, Jan. 2017, doi: 10.1016/j.jclepro.2016.03.126.

[88] G. Gereffi, J. Humphrey, and T. Sturgeon, "The governance of global value chains," *Rev Int Polit Econ*, vol. 12, no. 1, pp. 78–104, Feb. 2005, doi: 10.1080/09692290500049805.

[89] F. Costantino, G. Di Gravio, A. Shaban, and M. Tronci, "Smoothing inventory decision rules in seasonal supply chains," *Expert Syst Appl*, vol. 44, pp. 304–319, Feb. 2016, doi: 10.1016/j.eswa.2015.08.052.

[90] P. Yadav, P. Lydon, J. Oswald, M. Dicko, and M. Zaffran, "Integration of vaccine supply chains with other health commodity supply chains: A framework for decision making," *Vaccine*, vol. 32, no. 50, pp. 6725–6732, Nov. 2014, doi: 10.1016/J.VACCINE.2014.10.001.

[91] C. Jira and M. W. Toffel, "Engaging supply chains in climate change," *Manufacturing and Service Operations Management*, vol. 15, no. 4, pp. 559–577, Sep. 2013, doi: 10.1287/MSOM.1120.0420.

[92] B. K. Mishra, S. Raghunathan, and X. Yue, "Demand forecast sharing in supply chains," *Prod Oper Manag*, vol. 18, no. 2, pp. 152–166, Mar. 2009, doi: 10.1111/J.1937-5956.2009.01013.X.

[93] C. N. Verdouw, J. Wolfert, A. J. M. Beulens, and A. Rialland, "Virtualization of food supply chains with the internet of things," *J Food Eng*, vol. 176, pp. 128–136, May 2016, doi: 10.1016/J.JFOODENG.2015.11.009.

[94] L. B. Schwarz and H. Zhao, "The unexpected impact of information sharing on US pharmaceutical supply chains," *Interfaces (Providence)*, vol. 41, no. 4, pp. 354–364, Jul. 2011, doi: 10.1287/INTE.1110.0571.

[95] K. Rennings and C. Rammer, "The impact of regulation-driven environmental innovation on innovation success and firm performance," *Ind Innov*, vol. 18, no. 03, pp. 255–283, Apr. 2011, doi: 10.1080/13662716.2011.561027.

[96] J. Campbell, A. Goldfarb, and C. Tucker, "Privacy regulation and market structure," *J Econ Manag Strategy*, vol. 24, no. 1, pp. 47–73, Mar. 2015, doi: 10.1111/jems.12079.

[97] A. Goldfarb and C. E. Tucker, "Privacy regulation and online advertising," *Manage Sci*, vol. 57, no. 1, pp. 57–71, Jan. 2011, doi: 10.1287/mnsc.1100.1246.

[98] P. De Hert and V. Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?," *Computer Law and Security Review*, vol. 32, no. 2, pp. 179–194, Apr. 2016, doi: 10.1016/J.CLSR.2016.02.006.

[99] Y. Song, R. Routray, R. Jain, and C. H. Tan, "A data-driven storage recommendation service for multitenant storage management environments," *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, pp. 1026–1040, Jun. 2015, doi: 10.1109/INM.2015.7140429.

[100] Y. Gong, "Data consistency in a voluntary medical incident reporting system.," *J Med Syst*, vol. 35, no. 4, pp. 609–615, Aug. 2011, doi: 10.1007/s10916-009-9398-y.

[101] K. W. Pang and H. L. Chan, "Data mining-based algorithm for storage location assignment in a randomised warehouse," *Int J Prod Res*, vol. 55, no. 14, pp. 4035–4052, Jul. 2017, doi: 10.1080/00207543.2016.1244615.

[102] G. Rosano, F. Pelliccia, C. Gaudio, and A. J. Coats, "The challenge of performing effective medical research in the era of healthcare data protection," *Int J Cardiol*, vol. 177, no. 2, pp. 510–511, Dec. 2014, doi: 10.1016/J.IJCARD.2014.08.077.

[103] S. Son, S. Na, and K. Kim, "Product data quality validation system for product development processes in high-tech industry," *Int J Prod Res*, vol. 49, no. 12, pp. 3751–3766, Jun. 2011, doi: 10.1080/00207543.2010.486906.

[104] S. Purkayastha and J. Braa, "Big data analytics for developing countries-using the cloud for operational bi in health," *Electronic Journal of Information Systems in Developing Countries*, vol. 59, no. 1, pp. 1–17, Oct. 2013, doi: 10.1002/J.1681-4835.2013.TB00420.X.

[105] R. Zhao, Y. Liu, N. Zhang, and T. Huang, "An optimization model for green supply chain management by using a big data analytic approach," *J Clean Prod*, vol. 142, pp. 1085–1097, Jan. 2017, doi: 10.1016/j.jclepro.2016.03.006.

[106] L. Barabesi, A. Cerasa, D. Perrotta, and A. Cerioli, "Modeling international trade data with the Tweedie distribution for anti-fraud and policy support," *Eur J Oper Res*, vol. 248, no. 3, pp. 1031–1043, Feb. 2016, doi: 10.1016/J.EJOR.2015.08.042.