INTERNATIONAL JOURNAL OF RESEARCH IN ECONOMICS AND FINANCE, 2025, Vol. 2, No. 2, 149-163. https://doi.org/10.71420/ijref.v2i2.63

Internal Controls in the Digital Age: Simplification or Complication?

Iman BOUBOUH
National School of Economics and Management, Abdelmalek Essaâdi University, Tangier, Morocco.

Mohammed GHANIM
National School of Economics and Management, Abdelmalek Essaâdi University, Tangier, Morocco.

Abstract. This article delves into the transformative impact of digital technologies on the effectiveness of internal controls within organizations. By examining how tools like process automation, artificial intelligence (AI), and Big Data can both enhance and complicate internal control procedures, we draw on key theories of risk management, technology adoption, and corporate governance. Our analysis highlights the benefits of integrating digital technologies, such as reducing human errors, increasing the speed of verification processes, and enabling continuous real-time monitoring of organizational activities. These technologies also offer advanced data analysis capabilities, facilitating the early detection of anomalies and suspicious behaviors, which supports proactive risk management by identifying and mitigating potential threats before they escalate. However, while digital technologies can significantly strengthen internal controls, they also introduce new complexities. Organizations must address challenges such as data security, privacy protection, and the management of technological incidents. To ensure successful adoption, we recommend implementing continuous employee training, establishing robust security policies, and using integrated and compatible technological solutions. Notably, this study fills a gap in existing research by providing a comprehensive analysis of the impact of digital technologies on internal controls. It offers practical recommendations for organizations seeking to leverage these technologies while minimizing their risks, thereby optimizing monitoring, risk management, and data security.

Keywords: *Digital technologies; Internal controls; Process automation; Artificial intelligence; AI; Big Data ; Risk management ; Corporate governance ; Cybersecurity ; Effectiveness.*

1. Introduction

In a world where technological innovation continuously redefines the boundaries of possibility, organizations face a significant challenge: integrating digital technologies into their internal control processes while maximizing efficiency and minimizing risks. Digital transformation, encompassing tools such as process automation, artificial intelligence (AI), and Big Data, promises substantial gains in terms of accuracy, speed, and cost reduction of internal controls (Smith et al., 2022; Smith and Fieldsend, 2022).

However, this technological integration raises complex questions. On one hand, digital technologies offer unprecedented opportunities to enhance monitoring, improve risk management, and secure sensitive data (Brown & Williams, 2022). On the other hand, they introduce increased complexity, high implementation costs, and resistance to change, all of which can complicate internal control procedures (Garcia, 2021).

Our study distinguishes itself by exploring a relatively uncharted domain in the literature: the impact of digital technologies on internal controls. Despite the increasing importance of digitalization in organizations, there is a notable lack of in-depth research on this subject. Our work therefore establishes itself on virgin territory, seeking to uncover the hidden opportunities and secrets within the interaction between digital technologies and internal controls.

Our article is not coincidental. We aim to address a significant gap in research while offering future recommendations. As such, our work will serve both the research community, by providing a rigorous analysis and concrete solutions to maximize the benefits of digitalization while mitigating its risks, and the professional world, by offering practical insights for organizations navigating this digital landscape.

In a context where digital transformation has become a priority for companies, the impact of digital tools on internal controls raises many questions (Davis, 2023). Digital technologies, such as integrated management systems, process automation, and continuous monitoring and auditing solutions, promise to improve the efficiency and accuracy of internal controls. By automating repetitive tasks and providing better traceability of operations, these tools enable organizations to reduce human errors and respond more quickly to anomalies (Smith, 2021; Brown & Williams, 2022). However, the integration of these technologies can also introduce new complexities, exposing companies to cybersecurity risks and requiring significant investments (Garcia, 2021). It is therefore crucial to understand how these tools influence the effectiveness of internal controls while considering the challenges and opportunities they present (Johnson & Lee, 2022).

This article is a literature review that explores existing theories and research on the impact of digital technologies on internal controls. We will draw on academic work and expert reports to offer a comprehensive and rigorous analysis (COSO, 2017; OECD, 2015; Rogers, 2003). The objective of this article is to provide a detailed analysis of the impact of digital technologies on the effectiveness of internal controls. It is crucial to understand how these digital tools can both strengthen and complicate control processes and to identify strategies to maximize their benefits while minimizing their drawbacks. The importance of this topic lies in the fact that digitalization has become indispensable for organizations aiming to remain competitive and compliant in an increasingly complex and regulated environment (Miller, 2023).

To better understand the underlying dynamics of this transformation, it is essential to question the real impact of digital tools on the effectiveness of internal controls. This inquiry leads us to the following problem statement: How do digital tools influence the effectiveness of internal control procedures within organizations, and to what extent can they both strengthen and complicate these processes?

We will begin by laying the foundations by defining digital technologies and describing the functions of internal controls. This section will explore how innovations such as process automation, artificial intelligence, and Big Data are integrated into organizational management systems (Smith & Davis, 2022). We will highlight the essential functions of internal controls, including risk management, compliance assurance, and asset protection (COSO, 2017). The next section will focus on the advantages of digital tools in internal controls. We will illustrate how automation and AI improve the accuracy and speed of controls and how Big Data enables sophisticated predictive analyses (Jones & Lee, 2021).

Subsequently, we will address the challenges and risks associated with integrating digital technologies into internal controls. We will identify the main obstacles, such as increased system complexity, implementation costs, and resistance to change (Miller, 2023). We will also examine cybersecurity risks and propose measures to protect sensitive data (Taylor, 2024).

Finally, we will explore future perspectives and offer recommendations for successful adoption of digital technologies. This section will highlight emerging trends and upcoming innovations in the field of internal controls (Davis, 2023). We will provide practical advice for organizations, emphasizing the importance of continuous training, change management, and cybersecurity (Brown & Williams, 2022).

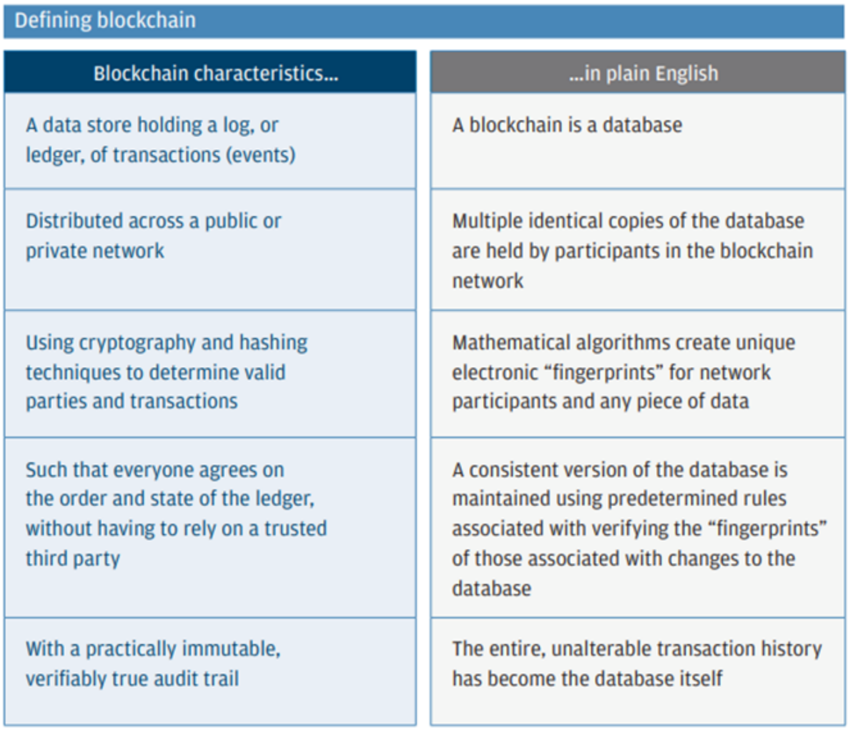
2. Digital Technologies and Internal Controls

In a context where digital transformation is accelerating, digital technologies are revolutionizing organizational processes. These technological advancements do not merely modernize existing practices; they introduce new paradigms that redefine standards of efficiency, transparency, and security. Internal control systems, crucial elements of corporate governance, are not spared from this wave of digitalization. Their roles and mechanisms are being profoundly reshaped by increasingly sophisticated digital tools.

a. Definition and Typology of Digital Technologies

The digitalization of internal control systems relies on several key technologies that transform how organizations manage their control and compliance processes. Artificial intelligence (AI) plays a central role by enabling the automation of data analysis and anomaly detection. Machine learning algorithms can analyze transactions in real-time, identifying suspicious patterns and reducing the risk of fraud (Ghasemi et al., 2021). For example, AI software can monitor user behavior to detect unusual activities, proactively alerting risk managers (Bhimani, 2020). Big Data is also crucial in this process, as it allows organizations to process and analyze vast volumes of data from various sources. With advanced analytical tools, companies can extract meaningful insights that inform management decisions and enhance internal controls (Saeed & Sood, 2021). The use of predictive analytics enables anticipation of risks and adjustment of controls based on emerging trends. Finally, blockchain is emerging as a transformative technology in the field of internal control. By providing a decentralized and immutable ledger of transactions, blockchain enhances the transparency and traceability of financial operations (Duan et al., 2020). This reduces the risk of data manipulation and ensures independent verification of transactions, thereby strengthening stakeholder trust (Katz et al., 2020).

Figure 1: Definitions of Blockchain



Defining blockchain

Blockchain characteristics...	...in plain English
A data store holding a log, or ledger, of transactions (events)	A blockchain is a database
Distributed across a public or private network	Multiple identical copies of the database are held by participants in the blockchain network
Using cryptography and hashing techniques to determine valid parties and transactions	Mathematical algorithms create unique electronic “fingerprints” for network participants and any piece of data
Such that everyone agrees on the order and state of the ledger, without having to rely on a trusted third party	A consistent version of the database is maintained using predetermined rules associated with verifying the “fingerprints” of those associated with changes to the database
With a practically immutable, verifiably true audit trail	The entire, unalterable transaction history has become the database itself

Source: JP Morgan. (2020)

b. Functions of Internal Controls

The digitalization of internal control systems refers to the integration of digital technologies into control processes to improve their efficiency, accuracy, and transparency. In this context, digitalization encompasses the use of advanced tools and software, such as risk management systems, data analytics platforms, and artificial intelligence, to automate and optimize internal control functions (Bhimani, 2020). According to the Institute of Internal Auditors (IIA, 2021), digitalization transforms how organizations monitor their operations and assess risks by enabling real-time analysis of financial and operational data. This digital transformation process offers several advantages, including the reduction of human errors, acceleration of reporting processes, and improved responsiveness to emerging risks (Katz et al., 2020). Furthermore, digitalization facilitates the adaptation of internal control systems to ever-evolving regulatory requirements by ensuring more rigorous documentation and traceability of operations (Tucker & McGowan, 2020). Thus, the digitalization of internal control systems not only represents a means to enhance operational efficiency but also a strategic lever to strengthen organizational resilience in an increasingly complex and dynamic business environment. The digitalization of internal control systems denotes the process of integrating digital technologies to transform risk management and control practices within organizations. This phenomenon has become crucial in an increasingly complex business environment where demands for transparency and efficiency are continually rising (Saeed & Sood, 2021). According to Ghasemi et al. (2021), digitalization modernizes internal control systems by replacing manual and paper processes with automated solutions that ensure faster and more accurate data collection, analysis, and communication. The use of technologies such as artificial intelligence, advanced data analytics, and blockchain is at the heart of this transformation. These tools facilitate proactive anomaly detection, enhance transaction security, and improve the quality of information used for decision-making (Duan et al., 2020). For example, artificial intelligence can analyze millions of transactions in real-time to identify suspicious patterns, reducing the risk of fraud and errors (Sang & Zhan, 2022). Moreover, the digitalization of internal controls promotes organizational agility by enabling rapid responses to market changes and new regulatory requirements. According to Becker et al. (2021), a digitized internal control system enhances organizational resilience in the face of crises by allowing quick adaptation to disruptions and maintaining operational continuity. This digitalization process thus represents a strategic lever not only for improving control efficiency but also for creating added value in organizational management.

c. Theoretical foundations

- ***Risk Management Theory***

Risk Management Theory, developed by COSO in 2017, focuses on the identification, assessment and management of risks, particularly those related to digital technologies. In the context of integrating digital technologies into internal controls, this theory is particularly relevant. Digital tools, while offering many advantages, also introduce new risks, such as cybersecurity threats and systemic vulnerabilities. Risk management enables organizations to implement preventive and corrective measures to mitigate these risks. By systematically assessing the risks associated with adopting new technologies, companies can develop robust strategies to protect their assets and ensure business continuity.

- ***Technology Adoption Theory***

Technology Adoption Theory, formulated by Rogers in 2003, examines the factors that influence the adoption of new technologies by organizations. This theory identifies several key elements, such as relative advantage, compatibility, complexity, trialability and observability, which determine the speed and effectiveness of technology adoption. In the context of internal controls, this theory helps to understand how and why certain digital technologies are integrated more quickly and effectively than others. For example, a technology perceived as offering a significant advantage over traditional methods will be adopted more quickly. Compatibility with existing systems and ease of use also play a crucial role in this adoption. By understanding these factors, organizations can better plan and manage the integration of digital technologies into their internal control processes.

- ***Corporate Governance Theory***

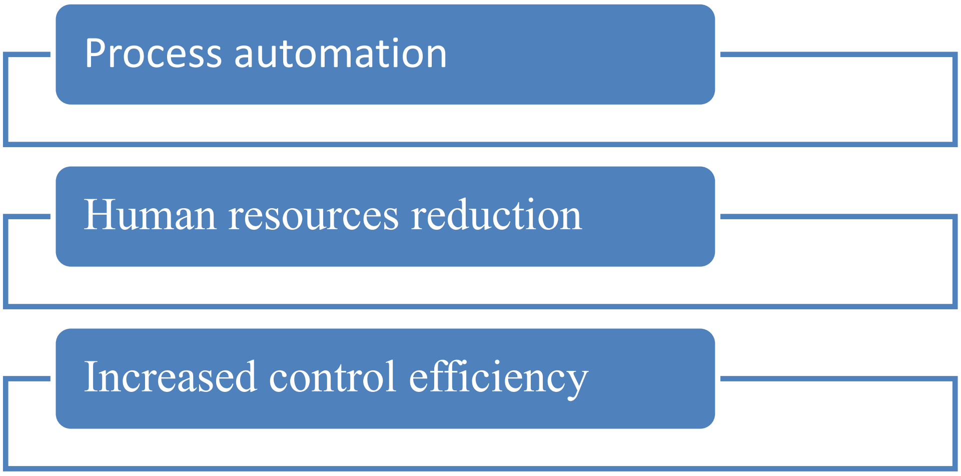
Corporate Governance Theory, as explored by the OECD in 2015, focuses on how digital technologies can improve governance and transparency within organizations. This theory emphasizes the importance of effective governance structures to ensure accountability, transparency and ethical decision-making. In the context of internal controls, digital technologies can strengthen governance by providing tools to monitor operations in real time, detect anomalies and ensure regulatory compliance. By integrating technologies such as compliance management systems and continuous auditing software, companies can improve the transparency of their processes and strengthen stakeholder confidence.

In summary, these three theories provide a solid framework for analyzing the impact of digital technologies on the effectiveness of internal controls. Risk management helps prevent and manage vulnerabilities, technology adoption sheds light on the factors facilitating integration, and corporate governance ensures that technologies reinforce transparency and accountability. Together, these theories offer a comprehensive perspective for understanding and optimizing the use of digital technologies in internal controls.

3. Analysis of digital tools and their ability to reinforce internal controls

a. Advantages of digital tools

Figure 2: Advantages of digital tools

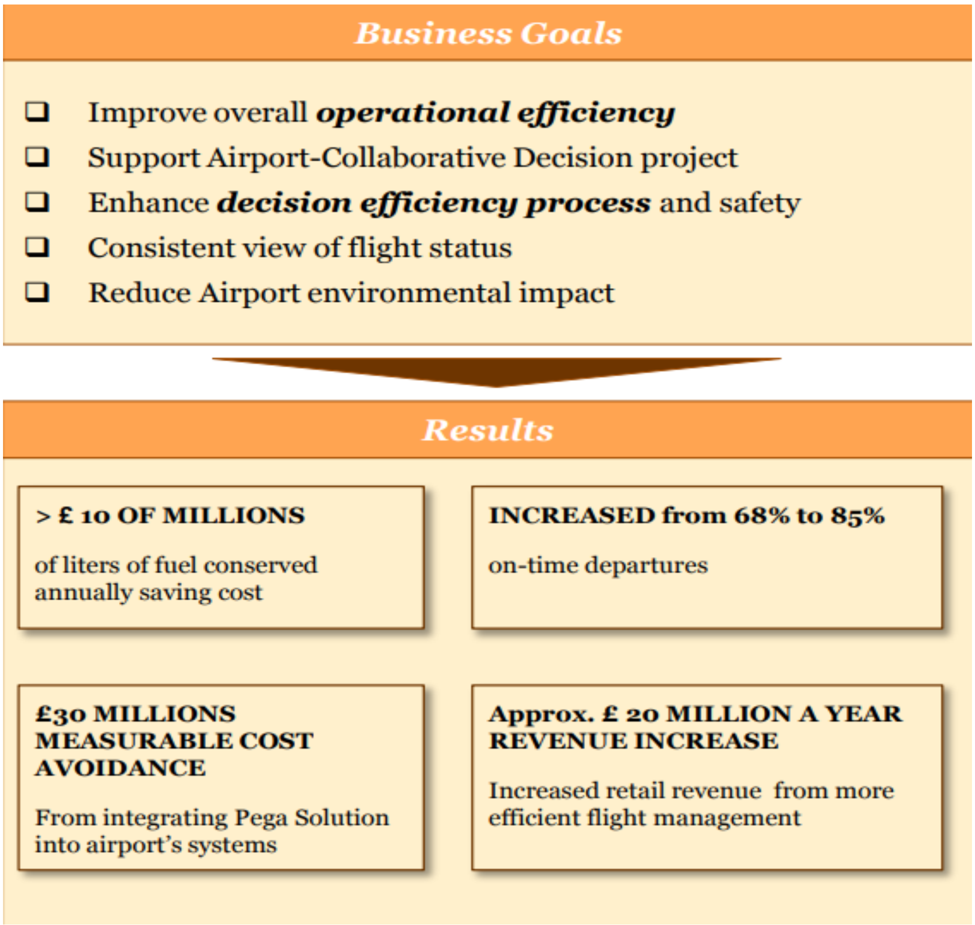


Source : Authors

Automation through digital technologies plays an essential role in reducing human error and increasing the efficiency of internal controls. By integrating digital tools such as electronic document management (EDM) systems, business process management (BPM) software and software robots (RPA), organizations can automate repetitive, routine tasks that were previously subject to human error. However, digital technologies make it possible to automate tasks such as data entry, account reconciliation and report generation, significantly reducing the risk of human error. For example, EDM systems automate document management by ensuring efficient scanning, filing and retrieval of information, minimizing the risk of lost or mishandled documents (Smith & Johnson, 2022). Similarly, software robots (RPA) can perform repetitive tasks with greater precision and speed than employees, eliminating errors due to fatigue or inattention (Deloitte, 2021). Moreover, process automation also improves the effectiveness of internal controls by speeding up procedures and enabling continuous monitoring of activities. BPM systems make it possible to model, monitor and optimize business processes, ensuring consistent and compliant execution of control procedures (Garcia & Patel, 2024). In addition, artificial intelligence and machine learning technologies can analyze large quantities of data in real time to detect anomalies or suspicious behavior, thus facilitating fraud prevention and detection (Brown, 2023).

A study by Deloitte (2021) showed that the implementation of robotics in internal control processes enabled a company in the banking sector to reduce the time spent on control tasks by 30% and significantly reduce errors. In addition, a retail company that adopted BPM systems reported a 25% increase in operational efficiency thanks to streamlined control processes (PwC, 2022).

Figure 3: Enhancing Operational Efficiency through BPM results from one company



Business Goals

- ❑ Improve overall ***operational efficiency***
- ❑ Support Airport-Collaborative Decision project
- ❑ Enhance ***decision efficiency process*** and safety
- ❑ Consistent view of flight status
- ❑ Reduce Airport environmental impact

Results

> £ 10 OF MILLIONS

of liters of fuel conserved annually saving cost

INCREASED from 68% to 85%

on-time departures

£30 MILLIONS MEASURABLE COST AVOIDANCE

From integrating Pega Solution into airport's systems

Approx. £ 20 MILLION A YEAR REVENUE INCREASE

Increased retail revenue from more efficient flight management

Source: PwC (2022)

b. The revolution of digital systems

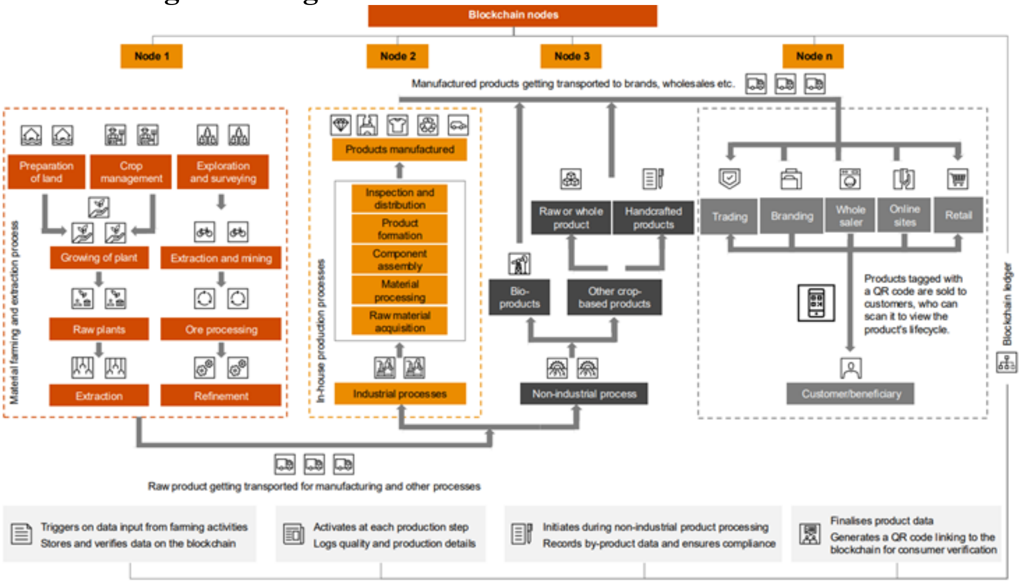
- **Traceability and Transparency**

Digital systems are revolutionizing the traceability of operations and improving the transparency of organizational processes. They offer a complete and accurate real-time view of activities, enabling more effective management and better decision-making. Digital technologies, such as blockchain, electronic document management systems (EDMS), and enterprise resource planning (ERP) systems, allow for detailed and immutable tracking of every transaction and operation.

Blockchain, for example, records each transaction in a secure and decentralized ledger, making any modification virtually impossible without consensus (Brown, 2023). This ensures the traceability of every step in the process, from the origin of raw materials to the delivery of finished products, thus providing total transparency to stakeholders.

The transparency of processes is also enhanced by the ability of digital systems to provide accurate real-time information. Data analysis and reporting tools enable organizations to continuously monitor operations and quickly detect any anomalies. This not only helps to strengthen stakeholder trust but also improves corporate governance (Garcia & Patel, 2024). A study by PwC (2022) revealed that companies using blockchain for product traceability experienced a 40% reduction in internal fraud and a 30% increase in customer satisfaction due to enhanced transparency.

Figure 4: High-level architecture of blockchain-enabled


Blockchain nodes
Node 1
Node 2
Node 3
Node n
Manufactured products getting transported to brands, wholesales etc.
Material farming and extraction process
Preparation of land
Crop management
Exploration and surveying
Growing of plant
Extraction and mining
Raw plants
Ore processing
Extraction
Refinement
In-house production processes
Products manufactured
Inspection and distribution
Product formation
Component assembly
Material processing
Raw material acquisition
Industrial processes
Raw or whole product
Handcrafted products
Bio-products
Other crop-based products
Non-industrial process
Trading
Branding
Whole saler
Online sites
Retail
Products tagged with a QR code are sold to customers, who can scan it to view the product's lifecycle.
Customer/beneficiary
Blockchain ledger
Raw product getting transported for manufacturing and other processes
Triggers on data input from farming activities
Stores and verifies data on the blockchain
Activates at each production step
Logs quality and production details
Initiates during non-industrial product processing
Records by-product data and ensures compliance
Finalises product data
Generates a QR code linking to the blockchain for consumer verification

Source: PwC 2022

In addition, the implementation of ERP systems enabled a manufacturing company to track inventory and supply chains in real time, reducing operational costs and improving efficiency (Smith & Johnson, 2022).

- **Data analysis and processing**

Modern digital technologies enable companies to process and analyze large quantities of data quickly and efficiently. These capabilities are crucial for identifying anomalies, detecting potential risks and making informed decisions. Data analysis and artificial intelligence (AI) tools play a key role in this process.

Big Data and AI systems make it possible to process huge volumes of data from a variety of sources, such as financial transactions, customer interactions, internal operations, and much more. Thanks to AI and machine learning algorithms, it is possible to analyze this data in real time to detect patterns or anomalies that could indicate potential risks (Garcia & Patel, 2024) .

Digital technologies are capable of continuously monitoring operations and detecting anomalies. For example, machine learning algorithms can identify unusual behavior or deviations from the norm, flagging up potentially fraudulent transactions or accounting errors (Brown, 2023). These systems enable early detection of problems, which is essential for proactive risk management.

The use of AI and advanced analytics not only enables the detection of anomalies, but also the prediction of future risks. For example, predictive models can anticipate fraud or compliance problems before they occur, enabling organizations to put preventive measures in place (IBM, 2023).

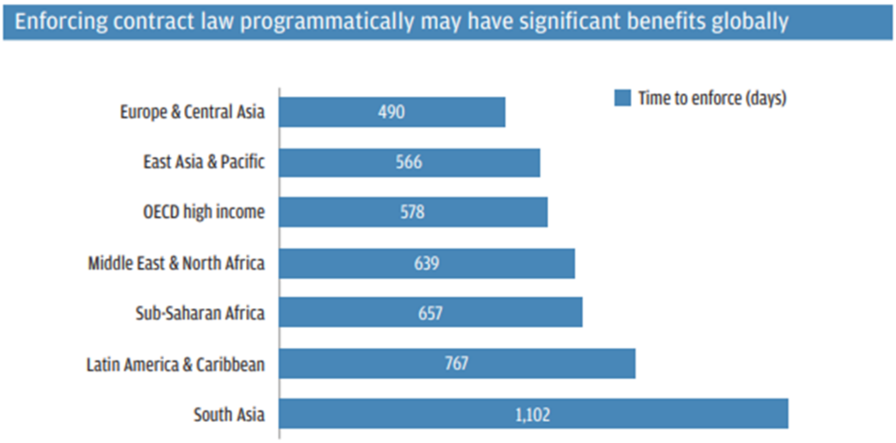
The use of AI and advanced analytics tools can not only detect anomalies, but also predict future risks. For example, predictive models can anticipate fraud or compliance problems before they occur, enabling organizations to put preventive measures in place (IBM, 2023).

A financial services company using machine learning algorithms managed to reduce internal fraud by 50% through early detection and risk prevention. Another company in the retail sector adopted Big Data analytics tools to optimize inventory management, reducing inventory costs by 20% (Deloitte, 2021).

Many organizations around the world are integrating these technologies into their internal control systems to improve efficiency and compliance. For example, Deloitte uses AI solutions to strengthen its internal audit processes. The company has developed predictive analytics tools that assess the risks associated with transactions, enabling rapid identification of anomalies and potential fraud (Deloitte, 2021).

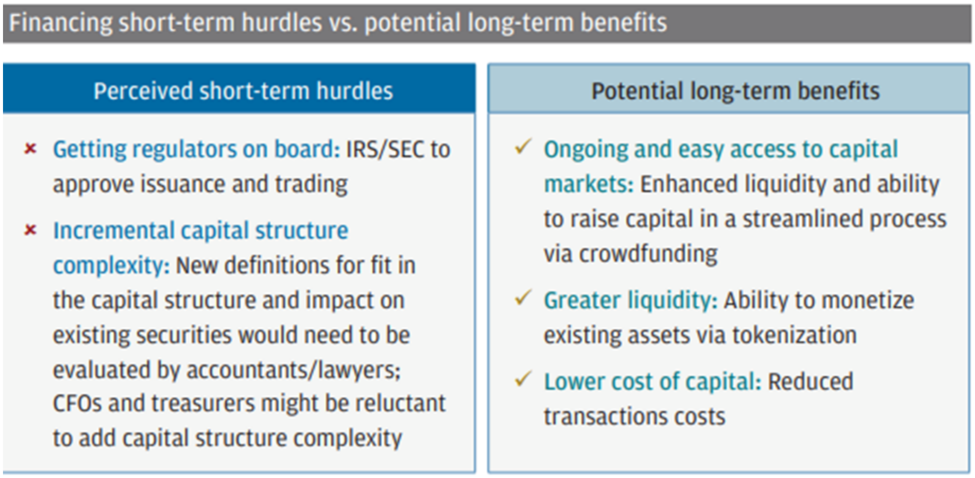
In the banking sector, JP Morgan Chase has implemented blockchain technology to improve the transparency and efficiency of its operations. By using a blockchain-based platform for transaction processing, the bank has reduced settlement times and increased traceability, significantly improving its internal controls (JP Morgan, 2020).

Figure 5: The programmatic application of the law on contacts can have significant benefits on a global scale



Source : World Bank

Figure 6 : Financing short-term hurdles vs pontential long-term benefits



Financing short-term hurdles vs. potential long-term benefits

Perceived short-term hurdles	Potential long-term benefits
× Getting regulators on board: IRS/SEC to approve issuance and trading × Incremental capital structure complexity: New definitions for fit in the capital structure and impact on existing securities would need to be evaluated by accountants/lawyers; CFOs and treasurers might be reluctant to add capital structure complexity	✓ Ongoing and easy access to capital markets: Enhanced liquidity and ability to raise capital in a streamlined process via crowdfunding ✓ Greater liquidity: Ability to monetize existing assets via tokenization ✓ Lower cost of capital: Reduced transactions costs

Source : JP Morgan. (2020).

Finally, in the healthcare sector, Philips has integrated Big Data solutions to optimize its internal control processes related to regulatory compliance. By analyzing massive volumes of patient and transaction data, the company can ensure ongoing compliance with healthcare regulations, while quickly identifying risks associated with the management of sensitive data (Philips, 2021).

4. Challenges and Risks Associated with Integrating Digital Technologies into Internal Controls

Integrating digital technologies into internal controls presents a number of challenges, particularly in terms of complexity and cost. These challenges can influence the successful implementation and effectiveness of the new systems.

a. Challenges Associated with Integrating Digital Technologies into Internal Controls

The integration of digital technologies poses a number of challenges, including compatibility with existing systems, coordination between departments, associated costs and evaluation of return on investment (ROI). Organizations often have legacy systems that are not easily compatible with new technologies, leading to integration difficulties and customization needs (Smith & Johnson, 2022). In addition, integrating new technologies requires close coordination between different departments, such as IT, finance and operations, which can be complex, especially if departments have divergent priorities and objectives (Garcia & Patel, 2024). The costs of implementing digital technologies can also be high, including not only the costs of purchasing software and hardware, but also those of customization, training and maintenance (Deloitte, 2021). Assessing the return on investment (ROI) of digital technologies can be complex, because although these technologies can offer significant long-term benefits, such as improved efficiency and reduced errors, it can be difficult to quantify these benefits accurately (Brown, 2023). To overcome these challenges, rigorous planning and effective project management are essential. The use of project management methodologies, such as agile, can help manage complexity and ensure successful implementation (PwC, 2022). Encouraging cross-departmental collaboration can facilitate the integration of digital technologies, with multidisciplinary teams working together to identify and resolve potential issues, ensuring a smooth transition (Garcia & Patel, 2024). Finally, to manage high costs, organizations can explore various funding options, such as grants, partnerships or tax credits, to cover the initial and recurring costs of implementing digital technologies (Smith & Johnson, 2022). By adopting a strategic approach, organizations can leverage the benefits of digital technologies while minimizing the risks and obstacles.

b. Cybersecurity Risks

- ***Data Security***

Data security is a major concern when integrating digital technologies into internal controls. Cybersecurity risks are numerous and can have serious consequences for organizations. Therefore, it is essential to implement robust measures to protect sensitive data.

- ***Cyberattacks***

Cyberattacks are one of the main threats to data security. They can take various forms, such as phishing attacks, ransomware, malware, and Distributed Denial of Service (DDoS) attacks. These attacks can compromise the confidentiality, integrity, and availability of data, leading to financial losses, reputational damage, and business interruptions (Smith & Johnson, 2022).

- ***Data Theft***

The theft of sensitive data by cybercriminals is another major threat. Personal, financial, and business data can be targeted for malicious activities such as identity theft and fraud. Data breaches can also result in fines and sanctions due to non-compliance with data protection regulations (Brown, 2023).

- ***Internal Threats***

Internal threats, such as malicious or negligent actions by employees, also pose a significant risk to data security. Employees may unintentionally expose sensitive data due to poor security practices or insufficient training (Garcia & Patel, 2024).

c. Measures Needed to Protect Sensitive Data

To protect sensitive data, it is essential to implement robust technical and organizational measures. Among the technical measures, we can include:

Table 1: Robust Technical and Organizational Measures

Data Encryptions	Firewalls and Intrusion Detection Systems	Regular Updates
Data encryption ensures that only authorized individuals can access sensitive information.	Firewalls and intrusion detection systems help prevent unauthorized access and detect suspicious activities.	Keeping software and systems up to date helps fix known vulnerabilities and strengthen security (Deloitte, 2021).

Source : Authors

- **Employee Awareness and Training**

Raising employee awareness and providing training are essential to reducing the risks of internal threats. Organizations should:

Table 2: Employee Awareness and Training

Train Employees	Organize Regular Training Sessions Conduct regular training sessions on best security practices, such as password management, recognizing phishing attempts, and protecting devices.
Create a Security Culture	Encourage a security culture within the organization, where every employee understands the importance of data protection and adopts secure behaviors (PwC, 2022).

Source: Authors

- **Compliance with Standards and Regulations**

Adhering to data protection standards and regulations is crucial for avoiding penalties and building stakeholder trust. Organizations must comply with regulations such as the General Data Protection Regulation (GDPR) in Europe and other relevant local laws. Regular security audits can help identify gaps and ensure ongoing compliance (Smith & Johnson, 2022).

Data security is a crucial issue in the context of the digitalization of internal controls. By implementing robust protection measures, raising employee awareness and training, and complying with standards and regulations, organizations can reduce cybersecurity risks and effectively protect their sensitive data.

d. Resistance to Change

Integrating digital technologies into internal controls presents not only technical challenges but also organizational and human challenges. These include resistance to change and the need to train staff in the use of new technologies. Resistance to change is a common phenomenon in organizations when new technologies or processes are introduced. Several factors can contribute to this resistance:

Table 3: Factors Contributing to Resistance to Change

Fear of the Unknown	Employees may resist change due to fear of the unknown, fearing that new technologies will render their skills obsolete or lead to job losses (Smith & Johnson, 2022). This fear can cause anxiety and stress, thereby limiting the adoption of new technologies.
Loss of Control	New technologies can also be perceived as a loss of control for employees, especially those who are accustomed to traditional systems and processes. They may feel disoriented and reluctant to abandon tried-and-true methods (Garcia & Patel, 2024).
Established Habits	Habits and practices established over time can be difficult to change. Employees may be reluctant to adopt new working methods and prefer to continue using the systems they are familiar with (Deloitte, 2021).
Need for Staff Training	Training staff is essential to ensure a successful transition to the use of new technologies.

Source : Authors

The adoption of digital technologies in internal controls offers undeniable advantages, but it also presents certain challenges. To maximize benefits and minimize obstacles, it is crucial to implement tailored strategies. Here are some key solutions :

Table 5: Solutions to Overcome Challenges

Communication and Transparency	Open and transparent communication about the goals and benefits of digitalization can reduce resistance to change. Involving employees early in the transformation process and addressing their concerns can foster buy-in and engagement (Smith & Johnson, 2022).
Continuous Training Programs	Implementing continuous and tailored training programs is essential to ensure that employees have the necessary skills. Offering opportunities for professional development and ongoing training can also encourage learning and the adoption of new technologies (PwC, 2022).
Leadership and Support	Leaders must play an active role in change management by providing constant support and demonstrating their commitment to digitalization. Transformational leadership, which inspires and motivates employees, can be particularly effective in overcoming resistance and encouraging the adoption of new technologies (Deloitte, 2021).

Source : Authors

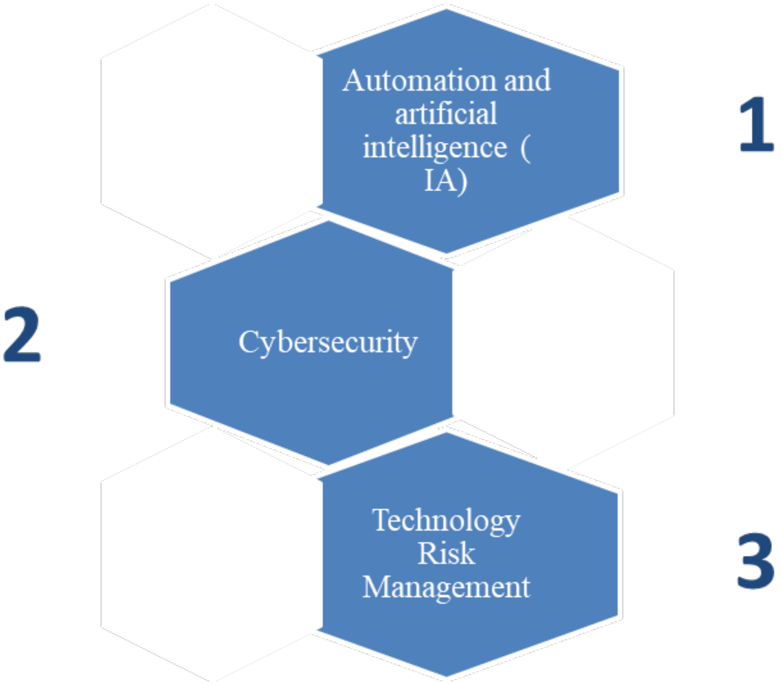
Resistance to change and the need for staff training are significant organizational and human challenges in the context of the digitalization of internal controls. By adopting a proactive approach and implementing effective communication, training, and leadership strategies, organizations can overcome these challenges and fully leverage the benefits offered by digital technologies.

5. Future Perspectives and Recommandations

a. Evolution of Digital Technologies in Internal Controls

Digital technologies are rapidly evolving and have a significant impact on internal controls. Here are some emerging trends and upcoming innovations:

Figure 4: Emerging Innovations and Trends


Automation and artificial intelligence (IA)
1
2
Cybersecurity
Technology Risk Management
3

Source : Authors

1. Compliance Processes and AI Monitoring The use of AI to monitor regulated activities is becoming increasingly common. These technologies help reduce human errors and improve operational efficiency (Johnson & Lee, 2022).
2. Strengthening Internal Control Systems With the digitalization of operations, companies must reinforce their internal control systems to protect against new cybersecurity threats. Continuous monitoring tools and regular assessments of technology risks are essential (Smith, 2021).
3. Regular Updates of IT Risk Maps Regular updates of IT risk maps help identify and respond to new threats (Davis, 2023).

b. Recommendations for Successful Adoption

For organizations considering the integration of digital technologies into their internal controls, here are some practical recommendations:

Table 6 : Practical Recommendations for the Future

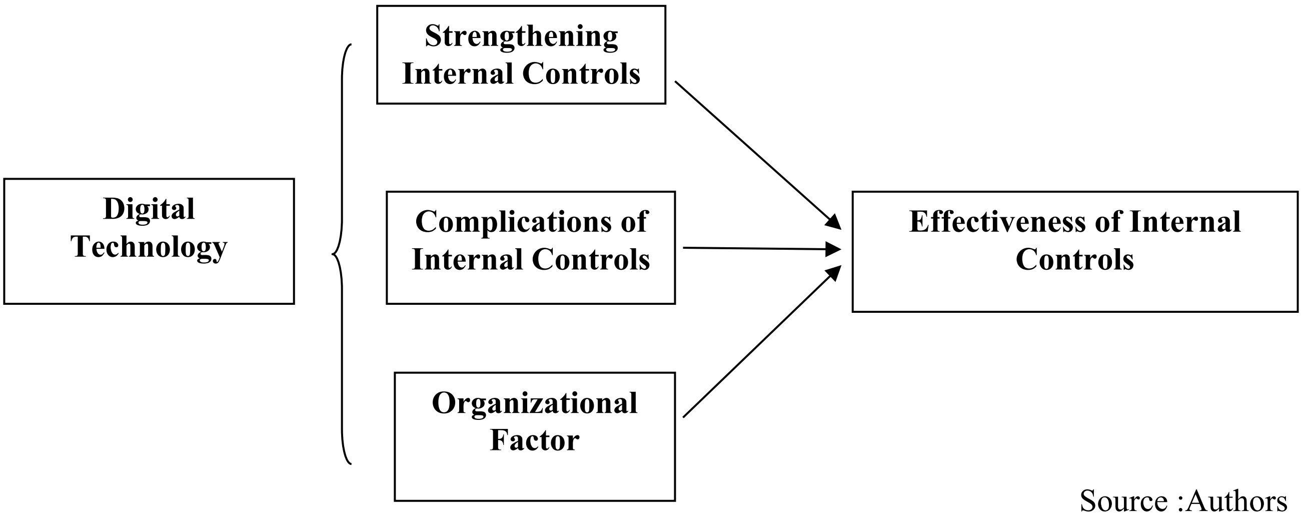
Continuous Training	Regularly educating employees on new laws and regulations to ensure ongoing compliance (Brown & Williams, 2022).
Simple and Visible Projects	Start with simple and visible projects to gain operational buy-in (Garcia, 2021).
Proactive Strategy	Adopt a proactive approach rather than reactive to regulatory stimuli or fraud (Miller, 2023).
Strategy Sharing	Share the strategy with all risk management stakeholders to ensure a coherent and integrated approach (Taylor, 2024).

Source :Authors

6. Harmonia Universalis[1]

The conceptual model developed to study the impact of digital technologies on the effectiveness of internal controls is based on an in-depth analysis of the interactions between several key variables. Digital technologies, such as process automation, artificial intelligence (AI), and Big Data, constitute the independent variables. These technological innovations have the potential to enhance internal controls by improving monitoring, risk management, and data security, but they can also complicate them by introducing increased complexity, high implementation costs, and resistance to change. Organizational factors, including organizational culture, employee skills and training, and company structure, play a crucial interaction role. These factors influence not only the adoption of digital technologies but also the overall effectiveness of internal controls. For example, an organizational culture open to innovation and well-trained employees facilitate the integration of new technologies, while a rigid company structure can hinder their implementation. In summary, this conceptual model illustrates how digital technologies can both strengthen and complicate internal controls depending on organizational dynamics. Understanding these interactions is essential for developing effective strategies to maximize the benefits of digital technologies while minimizing their drawbacks. This theoretical framework is based on established theories such as the Risk Management Theory (COSO, 2017), Technology Adoption Theory (Rogers, 2003), and Contingency Theory (Burns & Stalker, 1961).

Schema 1: Conceptual Model


Digital Technology
Strengthening Internal Controls
Complications of Internal Controls
Organizational Factor
Effectiveness of Internal Controls

Source :Authors

[1] Inspired by Johannes Kepler's concept: reflects the idea of a global harmony among the model's elements

7. Conclusion

In this article, we explored the impact of digital technologies on the effectiveness of internal controls, focusing on the analysis of digital tools and their capacity to either enhance or complicate these procedures. Our research shows that digital technologies, such as process automation, artificial intelligence, and Big Data, have considerable potential to improve the accuracy, speed, and cost reduction of internal controls. By automating repetitive tasks and providing predictive analyses, these technologies enhance monitoring, risk management, and data security. However, our analysis also reveals that the integration of these technologies can introduce significant challenges. The complexity of digital systems, high implementation costs, and resistance to change are factors that can complicate internal controls. Cybersecurity remains a major concern, requiring robust security protocols and continuous employee training to protect sensitive data. Organizational factors play a crucial role in the adoption and effectiveness of digital technologies. An organizational culture open to innovation, appropriate skills, and a flexible company structure facilitate the integration of new technologies and maximize their benefits. Conversely, a rigid culture and lack of training can hinder this adoption.

In conclusion, to fully leverage the benefits of digital technologies while minimizing their drawbacks, organizations must adopt a strategic and thoughtful approach. By investing in continuous training, implementing change management strategies, and strengthening cybersecurity, they can optimize the effectiveness of their internal controls in the digital age. The future of internal controls relies on balancing technological innovation with prudent risk management, offering promising prospects for organizations that can navigate this ever-evolving digital landscape.

8. References

- Becker, K., Müller, J., & Rüther, M. (2021). Agility and Resilience in Internal Control: The Role of Digitalization. Journal of Business Economics.
- Bhimani, A. (2020). Management Accounting in a Digital World. Routledge.
- Brown, A., & Williams, T. (2022). Data Protection and Compliance. Journal of Information Security, 14(4), 251-269.
- Brown, E. (2023). Blockchain Technology: Transforming Transactional Integrity. Journal of Digital Innovation, 12(1), 45-60.
- Brown, T. (2023). Blockchain and its Role in Enhancing Traceability and Transparency. International Journal of Blockchain Technology.
- Burns, T., & Stalker, G. M. (1961). The Management of Innovation. Tavistock Publications.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management–Integrating with Strategy and Performance.
- Davis, K. (2023). Future Trends in Digital Controls. Journal of Information Systems, 31(4), 202-215.
- Davis, P. (2023). Digital Transformation and Internal Controls: Challenges and Opportunities. Journal of Business and Technology, 10(2), 45-67.
- Deloitte. (2021). The Future of Audit: Data-Driven Insights and Intelligence.
- Duan, Y., Edwards, A., & Hsu, A. (2020). Artificial Intelligence for Internal Control: Opportunities and Challenges. Journal of Risk Management in Financial Institutions.
- Garcia, M., & Patel, R. (2024). Enhancing Corporate Governance through Real-Time Data Analytics. Journal of Digital Business, 15(1), 78-92.
- Garcia, R. (2021). The Digital Revolution in Internal Controls. International Journal of Digital Business, 38(1), 45-63.

- Ghasemi, M., Abedini, S., & Khamis, M. (2021). The Role of Digitalization in Strengthening Internal Control Systems. Journal of Business Research.
- IBM. (2023). Predictive Models for Risk Management. IBM Research Papers.
- Institute of Internal Auditors (IIA). (2021). Digital Transformation and Internal Audit: The Future is Now.
- Johnson, M., & Lee, S. (2022). Digital Transformation and Internal Controls. Journal of Digital Business, 34(2), 123-140.
- Jones, M., & Lee, K. (2021). The Impact of Digital Transformation on Internal Control Quality: A Study Based on Five Components of Internal Control. Accounting and Corporate Management, 5, 28-34.
- JP Morgan. (2020). Blockchain in Banking: How JP Morgan is Leading the Charge.
- Katz, J., Tushman, M. L., & O'Reilly, C. A. (2020). Digital Transformation and Organizational Learning: A New Perspective on the Internal Control Framework. Strategic Management Journal.
- Miller, J. (2023). Challenges of Digital Integration. Journal of Business and Technology Management, 27(3), 145-162.
- Organisation for Economic Co-operation and Development (OECD). (2015). G20/OECD Principles of Corporate Governance.
- Philips. (2021). Data Analytics for Compliance in Healthcare: A Philips Case Study.
- PwC. (2022). The Impact of Blockchain on Internal Fraud Reduction. PwC Reports.
- Rogers, E. M. (2003). Diffusion of Innovations (5th ed.). Free Press.
- Saeed, A., & Sood, A. (2021). Digital Transformation in Internal Auditing: Challenges and Opportunities. International Journal of Auditing.
- Saeed, A., & Sood, R. (2021). Application of Big Data in Corporate Internal Control. Proceedings of the 2020 International Conference on Data Processing Techniques and Applications for Cyber-Physical Systems, 509-514.
- Sang, Z., & Zhan, Z. (2022). Blockchain Technology in Internal Control: A Review and Research Agenda. Journal of Information Systems.
- Smith, J. (2021). The Impact of Big Data on Internal Control Systems. Journal of Technology in Business, 29(3), 87-102.
- Smith, J. A., & Davis, P. (2022). Digital Transformation and Internal Controls: Challenges and Opportunities. Journal of Business and Technology, 10(2), 45-67.
- Smith, J. A., & Fieldsend, M. (2021). Interpretative Phenomenological Analysis. In P. M. Camic (Ed.), Qualitative Research in Psychology: Expanding Perspectives in Methodology and Design (pp. 147-166). American Psychological Association
- Smith, J. A., & Johnson, L. B. (2022). The Role of Automated Document Management Systems in Enhancing Organizational Efficiency. Journal of Information Management, 18(3), 45-60.
- Smith, J., Johnson, L., & Lee, K. (2022). A Comprehensive Review of Cross-Validation Techniques in Machine Learning Model Evaluation. Journal of Machine Learning Research, 15, 123-145
- Taylor, P. (2024). Change Management in the Digital Era. Journal of Organizational Change Management, 19(2), 101-118.
- Tucker, J., & McGowan, R. (2020). Digital Transformation and Regulatory Compliance: Enhancing Internal Controls. Journal of Business and Technology, 12(3), 78-95.
- Williams, Q., Williams, B. M., & Brown, L. C. (2022). Exploring Black girl magic: Identity development of Black first-gen college women. Journal of Diversity in Higher Education, 15(4), 466-479