CYBER FRAUD, CORPORATE GOVERNANCE, AND CORPORATE SURVIVAL IN THE DIGITAL ECONOMY: STRATEGIES FOR BUILDING RESILIENT ORGANIZATIONS

Dr. SUNNY NWACHONIMUYA IKEOGWU
Department of Accounting
Faculty of Management sciences
University of Delta,Agbor Delta State
https://orcid.org/0009-0002-7720-547X
sunny.ikeogwu@unidel.edu.ng

Abstract

The increasing prevalence of cyber fraud in the digital economy poses significant challenges to organizational sustainability, making effective corporate governance essential for long-term corporate survival. This study examined the effect of corporate governance on corporate survival in the digital economy, with particular emphasis on internal control and risk management. A descriptive survey research design was adopted, and data were collected from 250 managerial and supervisory employees drawn from selected commercial banks, fintech firms, telecommunication companies, and insurance firms in Nigeria using purposive and simple random sampling techniques. A structured questionnaire based on a four-point Likert scale served as the instrument for data collection. The instrument was validated by experts, while reliability was established using Cronbach's Alpha. Data were analyzed using descriptive statistics and multiple regression analysis with the aid of SPSS Version 29 at the 5% level of significance. The findings revealed that internal control has a positive and statistically significant effect on corporate survival ($\beta = 0.436$, $t = 7.845$, $p < 0.001$), while risk management also exerts a significant positive influence on corporate survival ($\beta = 0.389$, $t = 6.974$, $p < 0.001$). The regression model explained 61.1% of the variation in corporate survival ($R^2 = 0.611$), indicating that corporate governance mechanisms play a substantial role in enhancing organizational resilience. The study concluded that robust internal control systems and proactive risk management practices are critical for minimizing cyber fraud, strengthening stakeholder confidence, ensuring operational continuity, and sustaining competitive advantage in the digital economy. The study recommends that organizations strengthen cybersecurity-oriented internal controls, integrate enterprise risk management into strategic decision-making, conduct regular cyber risk assessments, and invest in employee cybersecurity awareness programmes and advanced technological safeguards to enhance long-term corporate survival.

Keywords: Cyber Fraud, Corporate Governance, Internal Control, Risk Management, Corporate Survival, Digital Economy, Organizational Resilience.

Introduction

The digital economy has changed the way organizations create value, communicate with stakeholders, process payments, store information, and manage their internal operations. Businesses now depend heavily on online banking platforms, cloud-based applications, digital payment channels, electronic records, artificial intelligence, and interconnected supply chains. These developments have improved speed, convenience, and access to markets. At the same time, they have expanded the number of points through which fraudsters can attack an organization. Cyber fraud has therefore become a serious business concern rather than an issue that should be left only to information technology personnel. Cyber fraud refers to fraudulent activities carried out through computers, mobile devices, networks, digital platforms, or electronic communication systems. It may take the form of phishing, business email compromise, identity theft, ransomware, unauthorized

electronic transfers, manipulation of digital records, data theft, malware attacks, and insider misuse of organizational systems. The growing sophistication of these attacks means that organizations can suffer losses even where they have invested in modern digital tools. A recent systematic review by Liu and Babar (2024) shows that corporate cybersecurity risk has wide-ranging consequences, including operational disruption, financial losses, reputational damage, and weakened stakeholder confidence.

In a similar vein, Akujobi et al. (2026) observe that the rapid expansion of electronic payment systems in Nigeria has increased exposure to cyber fraud, especially where cybersecurity governance and regulatory implementation remain weak. The implications of cyber fraud go beyond the immediate loss of money or confidential information. A successful cyberattack can interrupt business operations, damage customer relationships, expose an organization to legal and regulatory sanctions, and reduce investor confidence. For organizations operating in highly competitive markets, repeated incidents may affect profitability, market value, and long-term survival. Ben (2026) argues that cybercrime can weaken corporate financial performance and reporting transparency by increasing recovery costs, reducing stakeholder trust, and placing pressure on governance and audit systems.

Thus, cyber fraud is increasingly linked to corporate survival because it affects the capacity of a firm to remain financially stable, operationally reliable, reputable, and sustainable over time. Corporate governance is central to how organizations respond to this challenge. Corporate governance concerns the structures, processes, and relationships through which organizations are directed, monitored, and held accountable. It includes board oversight, internal control, risk management, internal audit, ethical leadership, transparency, and compliance. In the context of cyber fraud, effective governance requires boards and senior managers to treat cyber risk as a strategic organizational issue. This means that cybersecurity should be integrated into enterprise risk management, internal audit planning, business continuity arrangements, and executive decision-making. Evidence from recent literature indicates that cybersecurity governance can strengthen investor and supply-chain trust and can also improve corporate market value (Zhang et al., 2025).

However, digital transformation does not automatically reduce fraud risk. While digital technologies can improve monitoring, detection, and reporting, they can also create new opportunities for fraud when systems are poorly governed. For instance, digital transformation may increase business complexity and oversight challenges, thereby making organizations more vulnerable to corporate fraud where internal controls and audit competence are inadequate (Wang et al., 2025). This suggests that the survival benefits of digitalization depend largely on the quality of governance arrangements surrounding it. Organizations must therefore combine technology investment with sound governance practices, staff awareness, effective access controls, fraud-reporting mechanisms, and well-tested incident-response plans. The need for resilient organizations has become more urgent because cyber threats continue to evolve. Fraudsters increasingly exploit human error, weak passwords, poorly protected devices, third-party vulnerabilities, and emerging technologies such as artificial intelligence and deepfakes.

Resilience, in this regard, is not simply the ability to prevent every attack; it is the ability to anticipate threats, withstand disruptions, respond quickly, recover effectively, and learn from incidents. Dwinanda and Utama (2025) emphasize that fraud-prevention outcomes are stronger when governance mechanisms combine structural oversight with ethical and organizational-cultural measures. Therefore, resilient organizations require not only technical safeguards but also accountable leadership, ethical conduct, continuous employee education, and strong internal control systems.

Against this background, this paper examines the relationship between cyber fraud, corporate governance, and corporate survival in the digital economy. Specifically, it discusses the nature and consequences of cyber fraud, explains the role of corporate governance in fraud prevention and control, and proposes strategies through which organizations can build resilience and sustain their operations in an increasingly digital business environment. The paper adopts a conceptual approach based on recent literature and secondary sources.

Objective

To examine the effect of corporate governance on corporate survival in the digital economy.

The specific are :

1. To examine the effect of internal control on corporate survival in the digital economy.
2. To determine the effect of risk management on corporate survival in the digital economy.

Research Questions

1. What effect does internal control have on corporate survival in the digital economy?
2. What effect does risk management have on corporate survival in the digital economy?

Research Hypotheses

H01: Internal control has no significant effect on corporate survival in the digital economy.

H02: Risk management has no significant effect on corporate survival in the digital economy.

Conceptual framwork

Concept of Cyber Fraud

Cyber fraud refers to deceptive, unlawful, or dishonest activities conducted through computers, mobile devices, internet platforms, electronic payment systems, or other digital communication channels for the purpose of obtaining money, personal information, organizational data, or other benefits unlawfully. Unlike traditional fraud, cyber fraud is often carried out remotely and may affect many individuals or organizations within a short period. It involves the deliberate use of digital technologies to manipulate, deceive, impersonate, steal, or gain unauthorized access to information and financial resources.

In contemporary organizations, cyber fraud has become more complex because business activities increasingly rely on electronic systems. Organizations use online banking, electronic payroll systems, cloud storage, enterprise resource planning systems, digital customer databases, social media platforms, and mobile applications to conduct daily operations. Although these technologies improve efficiency and reduce transaction costs, they also create opportunities for cybercriminals to exploit weaknesses in organizational systems. Cyber fraud may be committed by external attackers, employees, contractors, suppliers, customers, or organized criminal groups.

According to Liu and Babar (2024), cyber incidents and data breaches can create significant financial, operational, reputational, and legal consequences for organizations. Cyber fraud is therefore not limited to the theft of money; it may also involve the theft of sensitive customer information, intellectual property, trade secrets, passwords, and other confidential business data. Where such information is compromised, an organization may experience loss of customer trust, reduced competitiveness, litigation, regulatory sanctions, and disruption of normal business activities. One common form of cyber fraud is phishing. Phishing occurs when fraudsters send deceptive emails, messages, or links that appear to come from trusted organizations or individuals. The aim is usually to trick employees or customers into revealing passwords, banking details, verification codes, or other confidential information. Another common form is business email compromise, where criminals impersonate senior managers, suppliers, or business partners and instruct employees to make fraudulent payments. This type of fraud can be particularly damaging because it exploits trust and weaknesses in communication and payment approval processes. Identity theft is also a major form of cyber fraud. It occurs when criminals obtain and use another person's personal or financial information without authorization. In organizational settings, stolen identities may be used to access customer accounts, open fraudulent accounts, alter payment details, or carry out unauthorized transactions. Similarly, electronic payment fraud involves the unauthorized use of debit cards, credit cards, bank accounts, mobile money platforms, or online payment channels. The increase in digital financial services has made electronic payment fraud a growing concern for banks, businesses, and consumers. Another serious form of cyber fraud is ransomware. Ransomware is malicious software that blocks access to an organization's data or systems until a payment is made. In some cases, cybercriminals also threaten to release confidential data if the organization refuses to pay. Ransomware attacks can disrupt operations, delay service delivery, affect production activities, and expose organizations to financial and reputational losses. The increasing use of cloud systems and interconnected networks has made it important for organizations to develop effective backup systems, access controls, and incident-response procedures.

Cyber fraud may also arise from insider activities. Employees or other individuals with authorized access to organizational systems may misuse their privileges to steal information, manipulate records, divert funds, or assist external fraudsters. Insider cyber fraud is often difficult to detect because the individuals involved may understand the organization's procedures, controls, and system weaknesses. This makes internal control, segregation of duties, employee monitoring, ethical leadership, and whistleblowing mechanisms essential in reducing fraud opportunities. The consequences of cyber fraud can be severe for corporate survival. Organizations may lose money directly through fraudulent transactions or indirectly through recovery costs, legal expenses, system repairs, compensation to customers, and loss of business opportunities. Cyber fraud can also damage an organization's reputation, particularly where customers believe that their information is not secure. Wang et al. (2025) note that digital transformation can create additional fraud risks where governance systems, audit functions, and

internal controls do not develop at the same pace as technological adoption. Therefore, organizations must recognize that digitalization without effective governance can increase vulnerability to fraud.

In summary, cyber fraud is a multidimensional organizational risk that affects financial resources, information security, stakeholder confidence, and long-term business sustainability. It requires a coordinated response involving technology, corporate governance, internal audit, risk management, employee awareness, and ethical leadership. Organizations that fail to address cyber fraud may face serious threats to their continuity and survival in the digital economy.

Concept of Corporate Governance

Corporate governance refers to the system through which an organization is directed, controlled, and held accountable. It involves the rules, structures, policies, and relationships that guide decision-making within an organization. In practical terms, corporate governance explains who has the authority to make important decisions, how those decisions are monitored, and how managers are held responsible for their actions. It is concerned with ensuring that the interests of shareholders, employees, customers, creditors, regulators, and the wider society are fairly considered in the management of an organization. Corporate governance has become increasingly important in the digital economy because organizations now face risks that extend beyond traditional financial and operational concerns. Cyber fraud, data breaches, ransomware, identity theft, and unauthorized access to business systems can affect an organization's finances, reputation, customer confidence, and continuity.

As a result, governance is no longer limited to supervising financial reporting and executive behaviour. It now includes oversight of cyber risks, data protection, technology investments, and the organization's readiness to respond to digital threats. Liu and Babar (2024) observe that cybersecurity risk is a major corporate concern because cyber incidents can produce financial, operational, reputational, and regulatory consequences for firms. At the centre of corporate governance is the board of directors. The board is expected to provide strategic direction, monitor management activities, approve major policies, and ensure that adequate systems are in place to manage organizational risks. In relation to cyber fraud, the board should not treat cybersecurity as a purely technical matter for the information technology department. Rather, it should ensure that cyber risk is included in corporate strategy, enterprise risk management, internal audit planning, and business continuity arrangements. Board members must also receive clear and timely information about the organization's exposure to cyber threats, the effectiveness of existing controls, and the actions required to address identified weaknesses.

Another important governance mechanism is the audit committee. The audit committee supports the board by reviewing financial reporting, internal controls, audit findings, compliance matters, and risk-management practices. In the context of cyber fraud, the audit committee can help ensure that electronic transactions are properly monitored, access to sensitive systems is controlled, suspicious activities are investigated, and fraud risks are regularly assessed. A strong audit committee also encourages cooperation between internal auditors, external auditors, compliance officers, and information technology

personnel. This coordination is important because cyber fraud often involves both financial manipulation and technological compromise. Internal control is equally essential to corporate governance. Internal controls are the procedures and safeguards designed to prevent errors, detect irregularities, protect organizational assets, and ensure that operations are carried out according to approved policies. Examples include segregation of duties, approval limits, password controls, multi-factor authentication, regular reconciliation of accounts, access restrictions, audit trails, and independent reviews of sensitive transactions. Where these controls are weak, employees or external fraudsters may find it easier to manipulate records, divert funds, steal data, or gain unauthorized access to organizational systems.

Risk management is another key element of corporate governance. It involves identifying potential threats, assessing their likely impact, developing preventive measures, and preparing appropriate responses when risks occur. Cyber risk management requires organizations to identify their most valuable digital assets, assess vulnerabilities in their systems, monitor emerging threats, and establish procedures for responding to incidents. This may include data backup arrangements, incident-response teams, employee awareness programmes, vendor-risk assessments, and cyber-insurance considerations. The Three Lines Model is often used to clarify responsibilities: operational managers manage risks directly, risk and compliance functions provide oversight, while internal audit provides independent assurance on the effectiveness of controls (Tonti et al., 2024). Transparency and accountability are also central to effective governance. Transparency requires organizations to provide reliable and timely information about their operations, risks, and performance. Accountability means that individuals entrusted with authority can be questioned and held responsible for their decisions.

In cyber-fraud management, transparency may involve prompt reporting of material cyber incidents to the board, regulators, investors, and affected stakeholders where necessary. Accountability requires clear allocation of responsibility for cybersecurity, fraud prevention, data protection, and incident response. When responsibility is unclear, organizations may respond slowly to threats or fail to learn from previous incidents. Ethical leadership further strengthens corporate governance. Leaders who demonstrate integrity, fairness, and respect for organizational rules are more likely to create a culture in which employees report suspicious activities and avoid fraudulent conduct. Ethical leadership is particularly relevant to insider cyber fraud because employees with privileged access may misuse organizational information or systems when there is weak supervision, poor ethical culture, or little fear of sanctions. Fraud prevention is therefore more effective when formal governance structures are supported by a culture of honesty, openness, and responsible conduct. Recent reviews show that governance mechanisms such as board independence, audit committees, internal controls, audit quality, and transparency can reduce fraud risk, although their effectiveness may differ across industries, firm sizes, and regulatory environments (Apristiana & Utomo, 2025; Dwinanda & Utama, 2025). This means that organizations should not rely on a single governance mechanism. Instead, they should develop an integrated approach that combines board oversight, risk management,

internal audit, technology controls, employee training, ethical leadership, and effective reporting channels.

In summary, corporate governance provides the framework through which organizations manage cyber fraud and other digital risks. It helps to ensure that cyber threats are recognized early, controls are properly implemented, responsible officers are held accountable, and the organization is prepared to respond when incidents occur. In the digital economy, sound corporate governance is therefore a major requirement for protecting organizational resources, maintaining stakeholder confidence, and supporting long-term corporate survival.

Dimensions of Corporate Governance in Cyber-Fraud Control

Risk Management

Risk management refers to the systematic process of identifying, assessing, evaluating, monitoring, and responding to risks that may hinder an organization's ability to achieve its strategic objectives. Within the context of the digital economy, risk management involves the continuous identification and mitigation of cyber threats such as phishing attacks, ransomware, malware, identity theft, insider fraud, and business email compromise. Effective risk management ensures that organizations anticipate potential threats, implement preventive measures, and develop response strategies capable of minimizing operational and financial losses resulting from cyber incidents. As organizations become increasingly dependent on digital technologies, cyber risk management has become a strategic responsibility of corporate governance rather than merely a technical function of the information technology department. Contemporary organizations integrate cyber risk into enterprise risk management frameworks to strengthen resilience against emerging digital threats.

According to Liu and Babar (2024), organizations with mature cybersecurity risk management practices experience fewer operational disruptions and recover more effectively from cyber incidents because cyber risks are continuously monitored and incorporated into strategic decision-making. Recent empirical studies further demonstrate the importance of risk management in reducing cyber fraud and improving organizational sustainability. Zhang, Liu, and Chen (2025) found that organizations with effective cybersecurity governance and comprehensive risk management frameworks enjoy higher investor confidence and stronger market value because stakeholders perceive them as better prepared to manage cyber threats. Likewise, Akujobi et al. (2026) reported that Nigerian financial institutions with proactive cyber risk management practices recorded lower exposure to electronic fraud despite the rapid expansion of digital payment systems. Their findings emphasize that continuous risk assessment, employee awareness, regulatory compliance, and technological safeguards significantly reduce organizational vulnerability to cyber fraud. Risk management also strengthens corporate survival by enhancing organizational preparedness and resilience. It enables organizations to establish incident response plans, disaster recovery strategies, business continuity procedures, and continuous monitoring systems that minimize downtime during cyber incidents. Dwinanda and Utama (2025) observed that organizations adopting integrated governance mechanisms, including comprehensive risk management systems, are more capable of preventing fraud and maintaining long-term sustainability than organizations relying solely on technological controls.

Consequently, effective risk management enables organizations to withstand cyber threats, protect stakeholder interests, maintain operational continuity, and sustain competitive advantage in an increasingly uncertain digital environment.

Corporate Survival

Corporate survival refers to the ability of an organization to maintain continuous operations, achieve financial stability, adapt to environmental changes, and sustain competitive advantage over the long term despite internal and external challenges. In the digital economy, corporate survival extends beyond profitability to include organizational resilience, operational continuity, stakeholder confidence, adaptability, and the capability to recover quickly from cyber disruptions. Organizations that effectively manage technological risks and implement sound governance mechanisms are more likely to survive in environments characterized by increasing cyber threats and digital transformation. Corporate survival has become increasingly dependent on the quality of corporate governance because cyber fraud can significantly disrupt organizational activities. Cyber incidents often result in financial losses, operational interruptions, reputational damage, regulatory sanctions, and declining customer confidence.

According to Liu and Babar (2024), cyber incidents generate substantial operational, financial, legal, and reputational consequences that directly threaten the long-term sustainability of organizations. Consequently, organizations that fail to establish effective governance and cybersecurity practices face greater risks of declining performance and eventual business failure. Recent empirical evidence highlights the relationship between governance practices and corporate survival. Wang et al. (2025) found that organizations experiencing rapid digital transformation without corresponding improvements in governance structures and internal controls were more susceptible to corporate fraud, resulting in weaker financial performance and reduced organizational sustainability. Similarly, Zhang et al. (2025) demonstrated that effective cybersecurity governance enhances investor trust, strengthens supply chain relationships, and improves corporate market value, thereby contributing significantly to long-term corporate survival.

Furthermore, Dwinanda and Utama (2025) argued that governance mechanisms such as internal control systems, risk management practices, audit committee effectiveness, and ethical leadership collectively reduce fraud risk while improving organizational resilience and sustainability. In the Nigerian context, Akujobi et al. (2026) further observed that organizations implementing comprehensive cyber risk governance recorded better operational continuity and greater resilience against electronic fraud than organizations with weak governance structures.

Therefore, corporate survival in the digital economy depends largely on the ability of organizations to integrate effective internal controls and proactive risk management into their governance systems. These governance mechanisms strengthen resilience, protect organizational resources, sustain stakeholder confidence, and ensure business continuity despite the increasing sophistication of cyber fraud.

Accordingly, corporate survival remains an appropriate dependent variable for examining the effectiveness of corporate governance in addressing cyber threats in contemporary organizations.

Theoretical Framework

Agency Theory

Agency Theory was developed by Jensen and Meckling (1976). The theory explains the contractual relationship between principals (shareholders) and agents (managers), where managers are entrusted with the responsibility of managing organizational resources on behalf of owners. The theory argues that conflicts of interest often arise because managers may pursue personal objectives rather than organizational goals, particularly where monitoring mechanisms are weak. Such agency conflicts may result in fraud, misuse of organizational assets, poor decision-making, inadequate risk management, and weak accountability. Agency Theory emphasizes the importance of corporate governance mechanisms in aligning the interests of managers with those of shareholders. These governance mechanisms include effective internal control systems, risk management practices, board oversight, audit committees, transparency, and accountability. By establishing these mechanisms, organizations reduce opportunities for managerial opportunism, strengthen monitoring, improve accountability, and ensure that organizational resources are protected from fraud and abuse.

Within the digital economy, Agency Theory has become increasingly relevant because organizations rely heavily on digital technologies, electronic transactions, cloud computing, and interconnected information systems that expose them to cyber threats. Managers are expected to implement adequate cybersecurity policies, internal control procedures, and enterprise risk management systems to safeguard organizational assets against cyber fraud. Where governance mechanisms are weak, cybercriminals and even insiders may exploit system vulnerabilities, resulting in financial losses, reputational damage, operational disruptions, and reduced organizational performance. Internal control, one of the major governance mechanisms identified by Agency Theory, minimizes agency problems by establishing authorization procedures, segregation of duties, access controls, audit trails, continuous monitoring, and regular independent reviews. These controls reduce opportunities for fraud, improve financial reporting reliability, and ensure compliance with organizational policies. Likewise, effective risk management enables organizations to identify, assess, monitor, and mitigate cyber risks before they develop into significant threats capable of disrupting business operations.

Recent studies continue to support the relevance of Agency Theory in explaining the relationship between corporate governance and organizational sustainability. Liu and Babar (2024) observed that organizations with effective cybersecurity governance and monitoring systems experience fewer cyber incidents and recover more rapidly from digital disruptions. Similarly, Wang et al. (2025) found that firms undergoing digital transformation become increasingly vulnerable to corporate fraud where governance mechanisms and internal controls fail to keep pace with technological advancement. Dwinanda and Utama (2025) further reported that governance mechanisms such as internal control, audit effectiveness, and enterprise risk management significantly reduce fraud risk and improve organizational sustainability.

This theory is therefore appropriate for the present study because it explains how internal control and risk management, as corporate governance mechanisms, reduce cyber fraud, strengthen accountability, enhance operational resilience, and

ultimately improve corporate survival in the digital economy. Agency Theory provides the theoretical foundation for examining how effective governance practices contribute to the long-term sustainability and continuity of organizations facing increasing cyber threats.

Relevance of Agency Theory to the Study

Agency Theory underpins this study because it explains that effective corporate governance mechanisms—particularly **internal control** and **risk management**—are essential for reducing agency conflicts, preventing cyber fraud, protecting organizational assets, and ensuring corporate survival. The theory supports the argument that organizations with robust governance structures are better able to anticipate cyber risks, maintain stakeholder confidence, achieve operational continuity, and sustain long-term performance in the digital economy.

Empirical Review

Appah and Aganaba (2025) investigated the relationship between internal control effectiveness and business survival among listed firms in Nigeria, with leadership consistency serving as a moderating variable. The study adopted a cross-sectional research design using both primary and secondary data collected from 546 respondents across firms listed on the Nigerian Exchange Group. Data were analyzed using Structural Equation Modeling (SEM). The findings revealed that internal control effectiveness, measured through the control environment, risk assessment, control activities, information and communication, and monitoring, had a positive and statistically significant effect on business survival.

Furthermore, leadership consistency significantly strengthened the relationship between internal control effectiveness and business survival. The study concluded that organizations with effective internal control systems achieve higher productivity, organizational resilience, and long-term sustainability. Dao, Pham, and Xu (2024) examined the relationship between internal governance mechanisms and internal control quality using archival data from publicly traded firms. The study employed quantitative analysis to investigate whether effective internal governance reduces material weaknesses in internal control. The findings indicated that organizations with stronger internal governance structures were significantly less likely to report internal control material weaknesses, fewer recurring control deficiencies, and improved financial reporting quality. The study concluded that effective governance enhances organizational accountability and strengthens internal control systems, thereby improving organizational performance and long-term sustainability. The findings support the argument that internal control is an essential corporate governance mechanism for reducing organizational risk and enhancing corporate survival.

Amoah-Adjei and Taiwo (2025) examined whether risk governance predicts the survival of growth-stage firms in the United States. The study adopted a longitudinal research design using firm-level data from 2010 to 2023 and analyzed the data with the Cox Proportional Hazards Model. Risk governance was measured using board oversight quality, enterprise risk management (ERM) adoption, internal risk infrastructure, and innovation-oriented risk responsiveness. The results showed that firms with stronger enterprise risk management systems, effective board oversight, and robust internal controls had significantly lower risks of organizational failure and demonstrated greater long-term

survival. The authors concluded that proactive risk governance enhances organizational resilience by enabling firms to anticipate, mitigate, and recover from emerging business risks, including cyber threats.

Research Gap

Although previous empirical studies have established significant relationships between internal control, risk management, and organizational survival, most of these studies focused on general corporate governance practices or traditional business risks. Few studies have specifically examined internal control and risk management as dimensions of corporate governance in explaining corporate survival within the context of cyber fraud and the digital economy, particularly in developing economies such as Nigeria. This study therefore fills this gap by investigating how internal control and risk management influence corporate survival amid increasing cyber fraud challenges in the digital economy.

Methodology

This study adopted a descriptive survey research design to examine the effect of internal control and risk management on corporate survival in the Nigerian digital economy. The target population comprised managerial and supervisory employees of selected commercial banks, fintech firms, telecommunication companies, and insurance firms due to their extensive use of digital technologies and exposure to cyber fraud risks. A sample of 250 respondents was selected using purposive and simple random sampling techniques. Primary data were collected through a structured questionnaire comprising four sections: demographic information, internal control, risk management, and corporate survival. The instrument employed a four-point Likert scale ranging from Strongly Agree (4) to Strongly Disagree (1). The questionnaire was subjected to face and content validity by experts in Business Administration and Research Methodology, while its reliability was established using Cronbach's Alpha, with a minimum acceptable coefficient of 0.70. Data were analyzed using the Statistical Package for the Social Sciences (SPSS) Version 29. Descriptive statistics (frequency, percentage, mean, and standard deviation) were used to summarize respondents' characteristics, while multiple regression analysis was employed to test the hypotheses at the 5% level of significance.

The regression model is specified as:

$CS=\beta0+\beta1(IC)+\beta2(RM)+\varepsilon$CS = \beta_0 + \beta_1(IC) + \beta_2(RM) + \varepsilonCS=β0 +β1 (IC)+β2 (RM)+ε

Where:

- CS = Corporate Survival
- IC = Internal Control
- RM = Risk Management
- β_o = Constant
- β_1–β_2 = Regression coefficients
- ε = Error term

The functional relationship is expressed as:

CS=f(IC,RM)CS = f(IC, RM)CS=f(IC,RM)

This model assumes that effective internal control and risk management enhance corporate survival by strengthening organizational resilience, reducing cyber fraud risks, and improving operational continuity.

Results and Discussion

Descriptive Statistics

Table 1: Descriptive Statistics of the Study Variables (N = 250)

Variable	Mean	Std. Deviation
Internal Control	3.47	0.58
Risk Management	3.39	0.61
Corporate Survival	3.51	0.55

Source: Field Survey (2026)

Interpretation

Table 1 indicates that the respondents generally agreed that effective internal control (Mean = 3.47) and risk management (Mean = 3.39) are practiced within their organizations. The mean score for corporate survival (Mean = 3.51) also suggests that respondents perceived their organizations as resilient and capable of sustaining operations despite cyber-related challenges. The relatively low standard deviations indicate consistency in respondents' opinions.

Regression Analysis

Dependent Variable: Corporate Survival

Table 2: Model Summary

R	R^2	Adjusted R^2	Std. Error
0.782	0.611	0.607	0.392

Source: SPSS Version 29 Output (2026)

Interpretation

The model produced a correlation coefficient (R) of 0.782, indicating a strong positive relationship between corporate governance variables and corporate survival. The coefficient of determination ($R^2 = 0.611$) shows that 61.1% of the variation in corporate survival is explained by internal control and risk management, while the remaining 38.9% is attributable to other factors not included in the model.

Table 3: ANOVA

Source	Sum of Squares	df	Mean Square	F	Sig.
Regression	58.214	2	29.107	189.645	0.000
Residual	37.898	247	0.153		
Total	96.112	249			

Source: SPSS Version 29 Output (2026)

Interpretation

The ANOVA results indicate that the regression model is statistically significant (**F = 189.645; p < 0.001**). This confirms that internal control and risk management jointly predict corporate survival.

Table 4: Regression Coefficients

Variable	Beta	t-value	Sig.	Decision
Constant	0.845	4.182	0.000	
Internal Control	0.436	7.845	0.000	Significant

Risk Management	0.389	6.974	0.000	Significant

Dependent Variable: Corporate Survival
Source: SPSS Version 29 Output (2026)

Hypotheses Testing

Hypothesis One

H_{o1}: Internal control has no significant effect on corporate survival in the digital economy. The regression results show that internal control has a positive and statistically significant effect on corporate survival ($\beta = 0.436$, $t = 7.845$, $p < 0.001$). Therefore, the null hypothesis is **rejected**, and it is concluded that effective internal control significantly enhances corporate survival.

Hypothesis Two

H_{o2}: Risk management has no significant effect on corporate survival in the digital economy. The regression results indicate that risk management exerts a positive and significant influence on corporate survival ($\beta = 0.389$, $t = 6.974$, $p < 0.001$). Accordingly, the null hypothesis is **rejected**, indicating that effective risk management significantly improves corporate survival.

Discussion of Findings

The findings demonstrate that internal control significantly enhances corporate survival by strengthening organizational accountability, minimizing cyber fraud risks, and improving operational continuity. This finding supports the position of Appah and Aganaba (2025), who reported that effective internal control systems significantly improve business survival through enhanced governance and organizational resilience. The study further reveals that risk management has a significant positive effect on corporate survival. Organizations that proactively identify, assess, and mitigate cyber risks are better positioned to maintain business continuity and sustain competitive advantage. This finding is consistent with Amoah-Adjei and Taiwo (2025), who found that effective enterprise risk management and board oversight significantly improve long-term organizational survival by strengthening resilience against emerging business risks, including cyber threats.

Summary of Findings

The study examined the effect of corporate governance on corporate survival in the digital economy, with emphasis on internal control and risk management. The findings revealed that internal control has a positive and statistically significant effect on corporate survival. Organizations with effective internal control systems are better able to prevent cyber fraud, strengthen accountability, safeguard organizational resources, and maintain operational continuity. The study further established that risk management significantly enhances corporate survival by enabling organizations to identify, assess, and mitigate cyber risks before they adversely affect organizational performance.

Overall, the regression results demonstrated that corporate governance mechanisms jointly explain a substantial proportion of the variation in corporate survival, highlighting their critical role in building resilient organizations within the digital economy.

Conclusion

The study concludes that effective corporate governance is fundamental to

corporate survival in an increasingly digitalized business environment. Specifically, robust internal control systems and proactive risk management practices significantly improve organizational resilience by reducing exposure to cyber fraud, enhancing operational efficiency, and strengthening stakeholder confidence. As organizations continue to embrace digital technologies, governance mechanisms must evolve to address emerging cyber threats and ensure business continuity.

Therefore, organizations that institutionalize effective internal controls and comprehensive risk management frameworks are more likely to achieve long-term sustainability and maintain competitive advantage in the digital economy.

Recommendations

Based on the findings, the study recommends that:

1. Organizations should strengthen their internal control systems by implementing comprehensive cybersecurity policies, regular internal audits, segregation of duties, and continuous monitoring mechanisms to minimize cyber fraud and improve corporate survival.
2. Management should integrate enterprise risk management into strategic decision-making by conducting periodic cyber risk assessments, enhancing employee cybersecurity awareness, and investing in advanced technologies that improve organizational resilience and long-term sustainability.

References

Akujobi, C., Ogwueleka, F., Aimufua, G., & Bassey, S. (2026). *Cyber fraud in Nigerian banks: Trends, regulatory gaps, and mitigation strategies (2020–2025). Engineering and Technology Journal, 11*(1). https://doi.org/10.47191/etj/v11i01.18

Apristiana, A. A., & Utomo, D. C. (2025). *Corporate governance and fraud: A systematic review. Owner: Riset dan Jurnal Akuntansi, 9*(2), 703–725. https://doi.org/10.33395/owner.v9i2.2643

Ben, T. (2026). *Assessing the impact of cybercrime on corporate financial performance and reporting transparency in Nigeria: A policy and technological roadmap.* SSRN. https://ssrn.com/abstract=6277998

Dwinanda, R. R., & Utama, A. A. G. S. (2025). *The role of corporate governance in financial fraud prevention: A systematic literature review. Nominal: Barometer Riset Akuntansi dan Manajemen, 14*(2), 150–163. https://doi.org/10.21831/nominal.v14i2.81860

Liu, C., & Babar, M. A. (2024). *Corporate cybersecurity risk and data breaches: A systematic review of empirical research. Australian Journal of Management.* Advance online publication. https://doi.org/10.1177/03128962241293658

Valkenburg, B., & Bongiovanni, I. (2024). *Unravelling the Three Lines Model in cybersecurity: A systematic literature review. Computers & Security, 139*, 103708. https://doi.org/10.1016/j.cose.2024.103708

Wang, Y., Zhang, X., & Li, H. (2025). *Does digital transformation affect corporate fraud? Finance Research Letters, 80*, 107418.

https://doi.org/10.1016/j.frl.2025.107418

Zhang, Y., Liu, X., & Chen, H. (2025). *Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. Pacific-Basin Finance Journal, 90*, 102646. https://doi.org/10.1016/j.pacfin.2024.102646