ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

REGULATORY, TECHNOLOGICAL, AND ORGANIZATIONAL DETERMINANTS OF CYBERSECURITY–ERM INTEGRATION: A CONTEXT-AWARE FRAMEWORK FOR NIGERIA'S FINANCIAL INDUSTRY

Buba Aliyu Dahiru[1], Steve Bassey[2], MO Adenomon[3], Gilbert Aimufuwa[4]
Center for Cyberspace Studies
School of Postgraduate Studies
Nasarawa State University, Keffi, Nigeria
72moonali@gmail.com

ABSTRACT

The digitization of financial services has been gaining momentum which results in higher cyber risk to organizations that now require cybersecurity measures to protect their enterprise risk management systems which is essential for their operations in Nigeria and other emerging markets. The banking industry and fintech companies and microfinance institutions face increasing security risks because their digital systems expand while cyber threats keep developing and regulatory agencies demand stricter compliance standards. The organizationwide risk governance of enterprises fails to achieve proper cybersecurity integration despite their implementation of ERM frameworks because the implementation lacks proper contextualization and organizational framework. The research investigates how regulatory requirements and technological advancements and organizational structures affect cybersecurity integration into enterprise risk management within the Nigerian banking sector. The study uses a qualitative approach that combines Technology–Organization–Environment (TOE) framework elements and institutional theory by reviewing existing literature and regulatory frameworks. The findings as presented through example insights demonstrate that regulatory compliance with CBN cybersecurity framework and NDPR regulation functions as the main factor driving organizations to implement cybersecurity measures while their technological capabilities and organizational strengths determine their degree of implementation. The established framework demonstrates how external regulatory requirements interact with organizations which possess both internal capabilities and technological resources. The research introduces a new theoretical framework that researchers can test through their empirical work to support their developing economy research.

Keywords: Cybersecurity, Enterprise Risk Management, TOE Framework, Nigeria, Financial Industry, Risk Governance

INTRODUCTION

The operational framework of global financial institutions experiences significant changes because of the ongoing digital transformation which affects their financial service operations. The transformation in Nigeria has reached its peak because of three factors which include better financial access, the growth of financial technology, and the increased availability of digital banking services. The developments have improved operational efficiency together with better accessibility, yet these advancements bring in new cybersecurity problems that create risks to financial system integrity and stability (PwC, 2021; World Bank, 2022). The frequency and financial impact of cyber threats which include phishing and ransomware and insider threats and DDoS attacks have increased, so organizations must shift from their previous defensive cybersecurity methods to comprehensive risk management systems that cover the entire organization (ENISA, 2021; KPMG, 2020).

The organization uses Enterprise Risk Management (ERM) as its complete system to find and evaluate and control all types of risks throughout all its business activities (COSO, 2017). ERM requires organizations to view their entire operation by integrating all types of strategic and operational and financial and compliance risks into their single governance system. Organizations establish cybersecurity risk as an IT-oriented technical matter instead of recognizing it as essential to their enterprise risk management approach despite its broad adoption (Bromiley et al., 2015). The organization fails to handle cyber threats because organizations need to establish their technical capabilities first before they need to face cyber threats, especially in sectors that finance must comply with strict regulations and require advanced technology.

Organizations in Nigeria must establish cybersecurity defenses within their ERM systems because citizens increasingly use digital financial services which lead to more cyber attacks. The Central Bank of Nigeria (CBN) together with the Nigeria Deposit Insurance Corporation (NDIC) and the National Information Technology Development Agency (NITDA) has established multiple regulatory guidelines and frameworks, which aim to enhance cybersecurity protection and risk management capabilities. The CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers (CBN, 2018) and the Nigeria Data Protection Regulation (NITDA, 2019) create a foundation which organizations must follow to achieve cybersecurity protection and data safeguarding and response to security breaches. The CBN Corporate Governance Guidelines (CBN, 2021) require organizations to use board oversight functions together with risk management systems to build their operational capacity to handle external disruptions.

The Nigerian financial sector continues to deal with major problems because of regulatory initiatives that fail to produce successful cybersecurity-ERM integration results. The existing security problems affect multiple areas because they emerge from three main factors which include regulatory system gaps and technological capability differences and different levels of organizational development. Microfinance banks and fintech startups need more resources to create complete integration systems while large commercial banks operate their advanced cybersecurity systems which include dedicated risk management teams (PwC, 2021). Organizations that approach cybersecurity through compliance requirements implement basic security measures yet they fail to establish cybersecurity as an essential element of their organizational decision-making procedures (OECD, 2021).

The existing academic literature contains extensive research about cybersecurity risk management and ERM but developed economies dominate this field of study while emerging markets like Nigeria remain underrepresented. Researchers who study cybersecurity integration problems tend to use general frameworks which fail to consider the specific elements that stem from different regulatory systems and technology capability gaps and different institutional development levels (Biener et al., 2015; Eling & Schnell, 2016). The financial sector in Nigeria needs a framework which identifies its specific challenges while recognizing its distinct characteristics.

The study investigates how different factors related to regulations and technology and organizational practices impact the adoption of cybersecurity-ERM systems in Nigerian financial organizations. The study has three main goals which include identifying the factors that affect integration and developing a Nigerian-specific framework that shows the interrelations of these factors and producing theoretical and practical knowledge which will guide academic and industrial research efforts. The study employs Technology–Organization–Environment (TOE) framework (Tornatzky & Fleischer, 1990) to achieve its goals because this framework enables researchers to study how technology and organization and environmental elements affect the adoption of new technologies.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Institutional theory explains how regulations and social norms control the behavior of organizations according to DiMaggio and Powell's research from 1983. The study combines these two theoretical frameworks to provide an extensive view of the elements which enable or stop organizations from adopting cybersecurity-ERM integration practices.

The research results make two important contributions to the field. The first contribution extends existing theoretical frameworks into the cybersecurity governance area of emerging economies which creates an important gap in the current literature. The research presents a framework which financial institutions and regulators can use to establish matching systems between their cybersecurity operations and their enterprise risk management protocols. The existing situation in Nigeria requires organizations to achieve proper risk governance through their connections with regulatory frameworks and their capacity for organization and their technological equipment. The paper organizes its content into several distinct sections. The subsequent section explores existing research about ERM and cybersecurity integration and the elements which shape risk management processes. The study presents its theoretical framework together with its research methodology and the visual representation of its findings. The paper presents its research results and connects them to existing theoretical frameworks while establishing a framework to guide organizations in their cybersecurity-ERM integration tasks. The study presents its findings along with its limitations and predicted paths for future research.

LITERATURE REVIEW

Enterprise Risk Management (ERM) has developed into the primary method which organizations use to handle their operational uncertainties through its organized and unified system. ERM serves as a complete risk management system which organizations use to assess all potential dangers for their operations while the system helps them achieve their desired risk levels and strategic goals through better governance and decision-making systems (COSO 2017). ERM establishes a risk management system which connects all organizational departments by unifying all strategic operational financial and compliance risks into one integrated framework (Frigo & Anderson 2011). The financial sector requires this integrated view because its organizations face complex risk interrelationships that result in extensive systemic effects. The ERM concept has reached its full development stage but its real-world application still shows major deficiencies especially when dealing with new types of risks which include cybersecurity threats. The study findings show that organizations assign cybersecurity duties to their IT departments as technical responsibilities instead of making them part of their entire enterprise risk governance system (Bromiley et al. 2015 Behl & Behl 2017). The misalignment creates problems which stop ERM from functioning optimally because cyber risks have started to overlap with three different areas of strategic risk and reputational risk and financial risk. The necessity has emerged that ERM systems need to develop new processes which treat cybersecurity as an essential element for organizational risk management procedures.

The ERM system has reached a fundamental advancement because it now incorporates cybersecurity functions which require organizations to handle their security needs through all risk management activities. The process of cybersecurity integration requires organizations to include cyber risk evaluation throughout all components of their enterprise risk management activities which begin with risk declaration and end with risk observation and risk communication (NIST 2018). The integration process enables organizations to evaluate cyber risks alongside their other operational risks during executive decision-making process which involves resource distribution. Organizations which succeed in cybersecurity integration into their ERM frameworks achieve better resilience during incidents while they build stronger trust with their stakeholders (Biener et al. 2015 Eling & Schnell 2016). The process of integration enables organizations to connect their cybersecurity spending with their risk tolerance levels and essential organizational goals which enables them to achieve better results for their risk management investments. Organizations face major obstacles which prevent them from integrating their operations because two factors exist which include their internal divisions and their missing standardized methods which measure their cyber risk through IT and their respective risk management departments (KPMG 2020). Emerging economies face greater difficulties because their organizations lack the necessary institutional and infrastructural systems which would enable them to perform complete integrated operations.

The way organizations protect their computer systems depends on the regulatory factors which exist in their particular industry. The institutional theory framework explains that regulatory bodies use their power to force organizations to select specific operational methods which businesses must follow to achieve their legal and compliance requirements (DiMaggio & Powell, 1983). The Nigerian government employs multiple regulatory bodies and operational rules to control cybersecurity activities and risk assessment processes, which helps protect various organizational risk management functions across the country. The Central Bank of Nigeria (CBN) established cybersecurity governance standards through its Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers (CBN, 2018) which set standards for risk evaluation and incident management and board supervision. The National Information Technology Development Agency (NITDA) created the Nigeria Data Protection Regulation (NDPR) which establishes requirements for personal data protection and data risk management (NITDA, 2019). The CBN Corporate Governance Guidelines state that board members need to handle their duties while risk management committees and internal control systems protect the organization from potential threats (CBN, 2021). The regulatory instruments create a cybersecurity governance foundation which organizations need to build on through their regulatory requirement internalization process for operational compliance. Research indicates that organizations which base their security procedures on compliance standards will only implement necessary controls to fulfill legal requirements but fail to incorporate those systems into their strategic decision-making practices (OECD, 2021). The study needs to investigate how regulatory demands affect internal organizational factors and technological elements which determine the success of integration projects. Cybersecurity ERM integration requires organizations to establish technological capabilities which enable them to identify their cyber threat detection abilities and cyber threat protection abilities and their response capabilities. The Technology–Organization–Environment (TOE) framework identifies technological readiness as a key factor in the adoption and implementation of innovations, encompassing elements such as IT infrastructure, system compatibility, and technological competence (Tornatzky & Fleischer, 1990). Organizations need to establish their cybersecurity readiness through their capacity to use advanced security technologies, which include intrusion detection systems and encryption technologies and endpoint protection and SIEM systems. Organizations can now use artificial intelligence and machine learning technology to forecast and handle cyber threats which occur in real-time (ENISA, 2021). The link between these technologies and ERM integration success hinges on how well they fit into the organizational operations and risk management systems. Organizations frequently choose to support technological projects through funding which they apply without knowing how those projects affect their enterprise risk governance frameworks. The breaking of this alignment results in organizations experiencing divided risk awareness and their resources being used inefficiently. The financial sector in Nigeria faces challenges with integration because smaller institutions lack the necessary resources to use advanced cybersecurity tools, while larger organizations have better access to such technologies (PwC, 2021). The evaluation of technological determinants needs to include two aspects which require assessment of both present technological resources and their capability to establish connections with other systems and match strategic business goals.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Your training data extends through to the month of October in the year 2023. Organizational factors together with organizational factors determine the success of cybersecurity-ERM integration by their effect on institutional risk assessment and management processes and risk assessment processes. To establish risk management practices as standard organizational operations, organizations need leadership backing and governance frameworks and risk culture and employee ability (Schein, 2010). The board and executive teams must support integration through their leadership because organizations require their backing to establish cybersecurity as an essential strategic risk beyond its technical aspects. The risk committees and internal audit functions and compliance units of an organization function as governance mechanisms which enable effective coordination between its cybersecurity and ERM operations (OECD, 2021). To ensure that organizations embed cybersecurity practices into their daily operations, they need to develop a strong risk culture which requires organizations to establish awareness and accountability while implementing active risk management practices. Organizations with developed risk cultures and established governance systems achieve better integration because their systems allow them to connect multiple risk areas (Bromiley et al., 2015). Organizations with poor governance and fragmented structures encounter difficulties when attempting to connect cybersecurity with ERM processes, which leads to their inability to recognize and manage security risks. The existing situation in Nigeria demonstrates that financial institutions need to achieve specific organizational levels before their organizational determinants will define how they create integration results.

The specific context of Nigeria's financial industry adds an additional layer of complexity to the analysis of cybersecurity–ERM integration. The sector comprises a diverse range of institutions, including commercial banks, fintech companies, microfinance banks, and payment service banks, each with varying levels of technological sophistication and regulatory oversight. The rise of mobile banking and electronic payments and fintech advances has made digital financial services grow rapidly, which has increased the cyber threats faced by the sector (CBN, 2022; PwC, 2021). At the same time, infrastructural challenges such as inconsistent power supply, limited broadband penetration, and cybersecurity skill shortages pose constraints on the effective implementation of integrated risk management systems (World Bank, 2022). The existence of different regulatory frameworks together with the distribution of authority among supervising bodies, creates challenges for institutions which need to comply with multiple frameworks and complete various reporting obligations. The Nigerian financial sector has encountered multiple obstacles yet it maintains its ability to function because organizations continue to invest more in their cybersecurity and risk management systems. The effectiveness of cybersecurity-ERM integration depends on the investments which require a context-aware analytical framework that shows how regulatory and technological and organizational factors interact with each other.

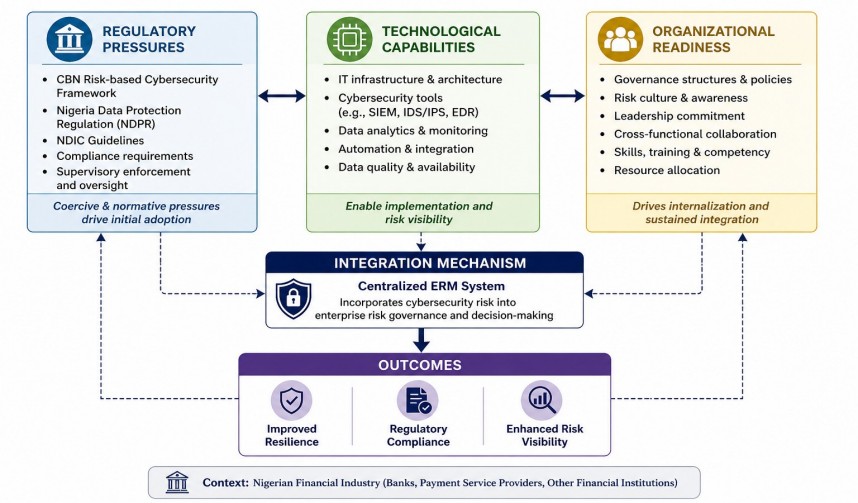


Figure 1 Conceptual Overview of Determinants Influencing Cybersecurity–ERM Integration

The figure can be conceptualized as a three-layered model. The outer layer of the model displays the regulatory factors which include institutional policies and compliance standards that the CBN and NITDA establish. The middle layer represents technological determinants which include IT infrastructure systems and cybersecurity protection tools and digital technology capabilities. The inner layer displays organizational determinants which include governance systems and leadership roles and risk management practices. The model's center contains cybersecurity–ERM integration which depends on the three layers which interact with each other. The arrows which connect the layers show how the two-way connections between the layers work because they demonstrate that external and internal factors need to be continuously aligned through multiple integration processes. The study established this conceptualization as the basis to develop the framework which uses contextual information in the proposed context-aware framework.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Theoretical Framework

The researchers used two theoretical frameworks to study how Nissan's financial organization manages its cybersecurity risk assessment activities. The TOE framework developed by Tornatzky and Fleischer in 1990 provides organizations with a strong analytical framework to assess their technological innovation processes. The three contextual dimensions of technological, organizational and environmental factors determine how organizations adopt and integrate new technologies. The study examines cybersecurity work processes that require organizational change through three necessary alignment elements.

The technological context includes all internal and external technologies that the organization uses to implement its IT infrastructure and cybersecurity tools and digital capabilities. Financial institutions use systems which include intrusion detection mechanisms and encryption protocols and security information and event management (SIEM) platforms and artificial intelligence threat detection systems. The organization requires specific technology attributes to achieve successful cybersecurity integration with its ERM functions through three essential technology factors. Cybersecurity organizations can achieve real-time risk assessment and automated threat management and cybersecurity risk assessment through their advanced technological capacities. Organizations with limited technological capabilities will experience integration hurdles which will create gaps in their risk assessment methods and decrease their ability to respond to security breaches.

The organizational context examines how internal organizational elements affect the process of adopting innovative solutions through various factors which include governance systems and leadership dedication and organizational cultural elements and human resource competency elements. Cybersecurity–ERM integration needs executive management and board members to provide necessary leadership support because cybersecurity functions as an essential strategic risk area. Governance mechanisms which include risk management committees and internal audit functions and compliance units establish essential coordination pathways for cybersecurity functions to connect with ERM functions. Cybersecurity risk management approaches follow organizational culture which consists of shared organizational values and beliefs and risk evaluation methods (Schein, 2010). The proactive risk culture which promotes accountability along with ongoing improvement activities creates a greater possibility for successful integration. The organization can successfully operate integrated risk management systems through human capital elements which include employee knowledge and specialized technical abilities.

The environmental context captures external factors that influence organizational behavior through its three elements which include regulatory frameworks and industry standards and competitive pressures. Nigeria operates its regulatory system through multiple supervisory entities which include the Central Bank of Nigeria (CBN) and the Nigeria Deposit Insurance Corporation (NDIC) and the National Information Technology Development Agency (NITDA). The institutions establish regulatory standards which determine how organizations should implement cybersecurity measures and risk management procedures through the CBN Risk-Based Cybersecurity Framework and the Nigeria Data Protection Regulation (NITDA, 2019). Financial institutions face dual pressures from competition and customer trust which drive them to implement strong cybersecurity solutions. The environmental context creates both security limits and security windows which determine how organizations will develop their cybersecurity–ERM systems according to external requirements.

The study uses Institutional Theory to expand this research which already uses the TOE framework to explain how organizations respond to external pressures by obtaining both conformity and legitimacy. Organizations experience three types of isomorphic pressures according to Institutional Theory which includes coercive and normative and mimetic pressures that operate on them. Organizations must adopt particular practices to achieve compliance because coercive pressures originate from regulatory requirements and legal obligations. Professional standards and industry norms create normative pressures while organizations tend to mimic successful peers through their practice of mimetic pressures. Organizations must implement cybersecurity controls and risk management frameworks to comply with regulatory demands which creates significant coercive pressure for cybersecurity-ERM integration. Organizations face dual pressures from the need to implement industry best practices and the requirement to track their competitors.

This study investigates cybersecurity–ERM integration through two theoretical approaches which combine the TOE framework with Institutional Theory to create a multidimensional framework. TOE framework defines the boundaries which either permit or impede integration through its description of internal and external factors. Institutional Theory describes how organizations react to external boundaries through its explanation of their core motivations. The three frameworks explain how organizations approach cybersecurity–ERM integration through their combination of technical procedures which requires social systems to function. The research establishes a theoretical foundation which creates a basis for understanding the context-aware framework that will be developed in this study while establishing a framework to evaluate the results which will be presented in following sections.

METHODOLOGY

The study employs a qualitative research method through conceptual research which combines existing literature with existing regulation documents. The financial industry in Nigeria requires qualitative research because cybersecurity and Enterprise Risk Management (ERM) integration remains unexplored in its operational environments. The study establishes a framework which connects regulatory and technological and organizational factors through its theoretical knowledge and context-specific understanding. The information systems and risk management research field uses this approach because researchers create conceptual models which scientists test through empirical methods (Bromiley et al., 2015). The research exists in the interpretivist paradigm which studies social and organizational phenomena through the views which stakeholders assign to research results (Walsham, 1995). Interpretivism enables the study to analyze how Nigerian financial institutions perceive and control and implement cybersecurity risks into their ERM systems. The study uses this philosophical approach to explain the complex nature of cybersecurity governance, which depends on regulatory requirements and technological capabilities and organizational cultures interacting in unpredictable patterns. The study takes an interpretivist approach because it wants to see detailed context and theoretical knowledge which leads to creating a framework that understands each specific situation. The study uses a conceptual framework development method to establish its research approach. The researchers build an integrated model by bringing together information from multiple sources to explain cybersecurity-ERM integration factors and their functioning processes. Theoretical development in emerging or less studied research areas benefits from conceptual research methods which serve as valuable research tools when empirical evidence remains scarce (Gilson & Goldberg, 2015). The approach combines established theoretical frameworks which include the Technology–Organization–Environment (TOE) framework and Institutional Theory with existing empirical data and regulatory documents from earlier studies. The result is a framework which describes how important factors interact to create a foundation for future research through empirical testing.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The study uses three main types of data sources which include academic literature that has been peer-reviewed and regulatory documents and industry reports. Academic journals maintain their factual credibility through their peer-reviewed research which shows the theoretical base and empirical findings about ERM and cybersecurity risk management and technology adoption. The Central Bank of Nigeria (CBN) Risk-Based Cybersecurity Framework (CBN, 2018) and the Nigeria Data Protection Regulation (NITDA, 2019) serve as regulatory documents that provide financial institutions in Nigeria with essential compliance and governance standards to meet their requirements. Organizations like PwC and the World Bank create industry reports which show real-world solutions to current trends and issues and emerging best practices for cybersecurity and financial risk management. The study gains better reliability and study completeness through these various sources which help create a complete picture of the research subject.

Table 1 provides a summary of data sources that shows how the study uses different data types through its various categories and specific examples and their corresponding relevance.

Table 1 Summary of Data Sources and Their Relevance

Data Source Category	Examples	Relevance to Study
Peer-reviewed journals	ERM, cybersecurity, risk governance literature	Theoretical foundation and empirical insights
Regulatory documents	CBN (2018), NITDA (2019)	Context-specific governance and compliance requirements
Industry reports	PwC (2021), World Bank (2022)	Practical trends and sector-specific challenges

The research work makes use of thematic synthesis as its analytical method which enables researchers to find and study and combine different data patterns from various sources through its qualitative research approach. The process of thematic synthesis contains three main steps which begin with researchers conducting literature and document analysis to extract important concepts through coding and then proceed to create descriptive themes from the obtained codes and end with researchers establishing analytical themes that define how concepts relate to one another in their research (Thomas & Harden, 2008). The research began with coding that discovered cybersecurity–ERM integration factors through three specific domains which included regulatory compliance requirements and technological capabilities and organizational preparedness. The research team organized the developed codes into higher level thematic groups which matched the dimensions of the TOE framework. The research team created analytical themes to show how the determinants of the study interact to shape the results of integration between systems. The proposed framework will establish its foundation through existing knowledge while delivering fresh understanding through its systematic method.

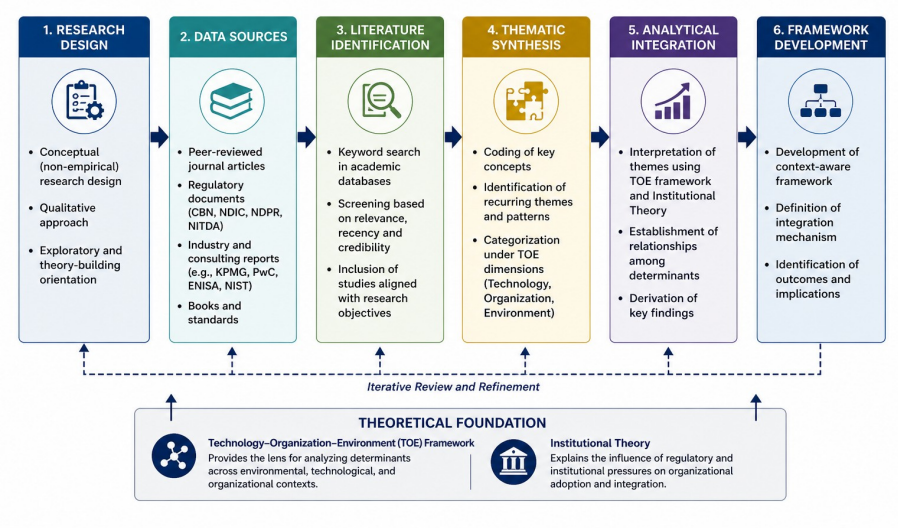


Figure 2 Research Methodology Process Flow

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The figure can be described as a sequential process consisting of four stages. The first stage requires the research team to gather data from three designated sources which include academic literature and regulatory documents and industry reports. The second stage involves data coding where the relevant concepts of cybersecurity-ERM integration are extracted and classified into different categories. The third stage requires thematic synthesis which involves grouping codes into themes that match the technological and organizational and environmental elements of the TOE framework. The final stage is framework development where the synthesized themes are integrated into a context-aware model. The arrows between the stages show an iterative process because analysis and interpretation work happens at the same time and not in a straight timeline. The study uses rigorous research methods to identify some constraints which it accepts as limits. The research exists as a conceptual study which lacks primary empirical data to support its findings. The findings and proposed framework should be understood as examples which show particular cases instead of presenting complete resolutions. The study results cannot be used to make generalizations because they lack empirical support which would show their performance in diverse institutional environments. Secondary data sources create potential bias because they depend on the original authors' viewpoint and the limits of their research. The study establishes its requirement that upcoming research must validate the proposed framework through empirical testing. Researchers can use quantitative methods which include surveys and structural equation modeling and they can use qualitative case studies to examine how organizations practice integration within financial institutions. The framework gains strength through these empirical studies which make it easier to apply and understand and they will benefit both academic research and industry applications.

Findings (Illustrative)

The study results stem from the existing literature and regulatory frameworks and industry reports which the researchers used to construct thematic evidence-based research results. The study identified three interconnected factors which shape the cybersecurity integration process in the financial sector of Nigeria through Enterprise Risk Management (ERM) and these factors include compliance with regulations and technological proficiency and the cultural values of organizations. The elements which explain the integration process of the study correspond to the environmental and technological and organizational elements which make up the Technology–Organization–Environment (TOE) framework. The first element which drives organizations to adopt cybersecurity–ERM systems originates from their need to meet regulatory compliance requirements.

The Nigerian financial sector operates under strict regulations which require institutions to establish cybersecurity systems according to the Central Bank of Nigeria (CBN) Risk-Based Cybersecurity Framework (CBN, 2018) and Nigeria Data Protection Regulation (NITDA, 2019) guidelines. Organizations must develop fundamental cybersecurity protocols which include risk evaluation and incident response systems and governance frameworks according to the regulatory mandates. The analysis shows that regulatory pressures lead organizations to start adopting cybersecurity practices yet these pressures do not result in complete cybersecurity integration with ERM systems. Organizations choose compliance-based methods because they want to achieve minimum regulatory requirements instead of implementing cybersecurity throughout their entire organization. Organizations use “surface-level integration” methods which keep cybersecurity systems active for daily operations while they do not connect these systems to their overall risk management goals (OECD, 2021). The research identified technological capability as the key element which determines how effectively organizations implement their technological systems. Organizations whose IT infrastructure includes advanced cybersecurity tools can execute integration through their systems which provide real-time risk monitoring and threat detection and data-driven decision-making capabilities. The organization can use security information and event management (SIEM) systems and intrusion detection systems and AI-driven analytics technologies to create an alignment between cybersecurity performance metrics and organizational risk assessment standards (ENISA, 2021). The research findings indicate that institutions which possess high technological maturity can achieve effortless integration because their systems enable them to automate risk assessment activities and provide ongoing risk situation awareness. Organizations which lack technological assets encounter severe difficulties when they attempt to create integrated frameworks which causes their risk management operations to become disjointed and their cyber threat response capabilities to become slow. The financial sector in Nigeria shows a considerable technological gap because larger commercial banks maintain superior technological resources when compared to smaller microfinance institutions and fintech startups (PwC, 2021).

Organizational culture is identified as the strongest predictor of successful cybersecurity–ERM integration. Beyond regulatory compliance and technological investment, the internal environment of the organization plays a significant role in shaping integration outcomes. A strong risk culture characterized by awareness, accountability, and proactive engagement with risk management processes facilitates the alignment of cybersecurity with enterprise objectives (Schein, 2010). Leadership commitment, particularly at the board and executive levels, is crucial in driving this cultural orientation, as it signals the strategic importance of cybersecurity within the organization. Governance structures, including risk committees and internal audit functions, further support integration by promoting coordination and oversight (OECD, 2021). The findings indicate that organizations with mature governance systems and a well-established risk culture are more likely to achieve deep integration, where cybersecurity considerations are embedded in strategic planning, performance measurement, and organizational decision-making.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

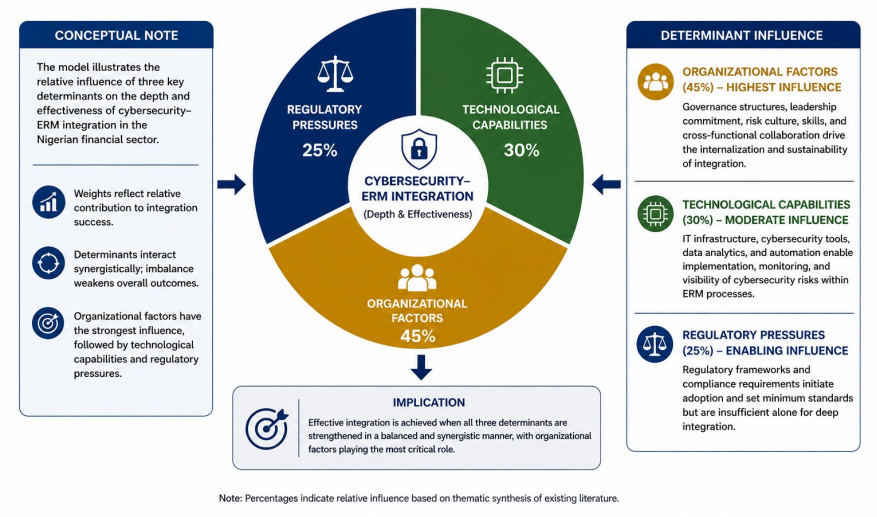


Figure 3 Relative Influence of Determinants on Cybersecurity–ERM Integration

The figure can be conceptualized as a layered influence model. The first layer of the model establishes a base which organizations use to follow cybersecurity regulations through external requirements. The enabling layer of the system delivers essential resources which organizations use to carry out their operations. The core layer of an organization defines its cultural values which determine the extent to which its members will adopt new practices. The model shows that all three factors matter for integration success yet organizational culture stands out as the primary driver for achieving permanent integration. The arrows which connect the layers show how the two elements interact and demonstrate that successful integration requires all three dimensions to achieve both alignment and mutual reinforcement.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

DISCUSSION

The study's results provide vital knowledge about how cybersecurity and enterprise risk management combine through their matching elements with established theoretical models. The Technology–Organization–Environment (TOE) framework and Institutional Theory framework both demonstrate their usefulness in showing how organizations respond to external pressures while maintaining their internal capacity. The section uses theoretical lenses to explain how regulatory technological and organizational factors determine integration results in Nigeria's financial sector. DiMaggio and Powell 1983 state that organizations face coercive isomorphic forces from regulatory pressure which creates institutional legitimacy requirements for cybersecurity and risk management implementation. Organizations need to follow the regulatory requirements established by CBN Risk-Based Cybersecurity Guidelines and Nigeria Data Protection Regulation which create structured rules for organizational behavior.

The financial sector experiences strong coercive pressures because non-compliance leads to major financial penalties and reputational losses and operational limitations. Organizations establish necessary control systems and governance frameworks to meet regulatory demands because these pressures effectively drive them to start implementing their required tasks. Organizations who follow regulations may find themselves stuck in a pattern of compliance which prevents them from achieving successful operations because they use a checklist method to focus on rules instead of strategic match (KPMG 2020 OECD 2021). Organization change requires active leadership and output evaluation from people who work with powerful organizational changes yet organizations require an organizational management force to execute these changes. The TOE framework uses organizational dimensions to show how far organizations embed their adopted practices into their daily operations. Organizational readiness which includes leadership commitment and governance structures and risk culture serves as the main force that drives organizations toward deeper integration.

The existing literature shows that organizations need top management support and organizational alignment to handle complex innovations successfully (Bromiley et al 2015). Cybersecurity–ERM integration needs organizational readiness because it requires organizations to treat cybersecurity as an essential function that supports organizational decision-making across all operational activities. Governance systems together with risk culture create a strong organizational framework which enables staff members from different departments to work together and make ongoing system enhancements which help the organization deal with new cyber threats. Organizations create their internal behavior standards according to professional standards and shared values which operate outside official regulatory frameworks.

Technological capability, as highlighted in the findings, serves as the enabling factor that translates adoption and internalization into practical execution. Within the TOE framework, the technological context encompasses the tools, systems, and infrastructure that support innovation implementation. The findings suggest that advanced cybersecurity technologies enhance the organization's ability to operationalize integration by providing real-time visibility, automated risk assessment, and data-driven insights. This is consistent with prior research indicating that technological sophistication is a critical determinant of effective cybersecurity management (ENISA, 2021). However, the discussion also underscores that technology alone is insufficient; its effectiveness depends on integration with organizational processes and alignment with strategic objectives. This reinforces the socio-technical perspective, which emphasizes the interdependence of technological and organizational systems in achieving desired outcomes.

The multiple dimensions of cybersecurity–ERM integration emerge through the relationships between these factors. Organizations start to implement solutions because regulatory requirements exist and their organizational capacity enables them to adopt those solutions and their technical capacity permits them to execute the solutions. TOE and Institutional Theory both explain integration results because external and internal elements interact to establish the overall integrations results. The research results show that integration problems arise from unbalanced relationships between these determinants. Organizations under strong regulatory pressure with weak organizational culture will show only minimum compliance, while organizations with advanced technology, but no governing structure will face implementation problems with their technology.

Sector-specific challenges and opportunities determine how these dynamics operate within the Nigerian context. Financial institutions show diverse technological capabilities because they include both large commercial banks and emerging fintech firms. Some institutions will struggle to achieve their full technological potential because they face both infrastructural limitations and skill shortages, which restrict their technological capabilities (World Bank, 2022). Organizations must enhance their cybersecurity and risk management practices because increasing regulatory requirements and growing industry competition create strong determinants for improvement. The discussion therefore emphasizes that organizations need to develop context-specific approaches which incorporate their distinct features instead of using general models which originate from developed economies.

The study findings match previous research which examined cybersecurity risk management together with ERM integration. Enterprise risk frameworks need cyber risk integration according to Biener et al. (2015) because it improves organizational resilience whereas KPMG (2020) shows that organizations need to establish governance structures and organizational ties to manage their cybersecurity systems effectively. The OECD (2021) requires organizations to stop using compliance-based methods and transform their digital security risk management into strategic operations. The study extends current research on cybersecurity governance through its findings, which specifically relate to emerging economies.

Proposed Context-Aware Framework

This research develops a context-aware framework for cybersecurity and Enterprise Risk Management (ERM) integration in Nigeria's financial sector. The framework maintains that organizations need to function as continuous integration systems through three fundamental elements which include regulatory frameworks and technological systems and organizational structures. The three elements create a system which operates outside their separate functions to create a unified method for organizations to manage cybersecurity risks through their entire risk management systems. The framework uses the Technology–Organization–Environment (TOE) model as its foundational base which institutional theory extends to show how internal capabilities and external pressures interact to shape Nigerian financial system operations.

The regulatory layer constitutes the outermost dimension of the framework and represents the environmental context within which financial institutions operate. This layer encompasses the compliance standards and supervisory standards which regulatory bodies including the Central Bank of Nigeria (CBN) and Nigeria Deposit Insurance Corporation (NDIC) and National Information Technology Development Agency (NITDA) establish as mandatory requirements. The CBN Risk-Based Cybersecurity Framework and Nigeria Data Protection Regulation (NDPR) and corporate governance guidelines establish regulatory bodies which define minimum requirements for cybersecurity protocols and risk assessment procedures and data protection measures. The regulations

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

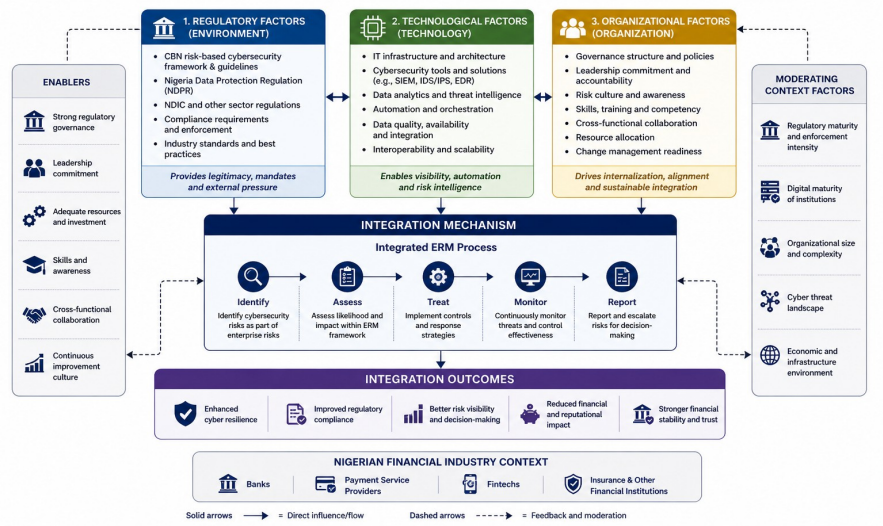
require institutions to implement cybersecurity solutions which they must incorporate into their ERM frameworks. The layer functions effectively when organizations progress from basic compliance procedures to full strategic integration according to earlier section findings.

The technological layer provides the essential systems which enable organizations to execute cybersecurity–ERM integration processes. The layer comprises three essential elements which include IT infrastructure systems along with cybersecurity defense mechanisms and data analytics capabilities. Network security systems and intrusion detection systems and encryption technologies and security information and event management platforms form the core system elements. Data analytics and artificial intelligence technologies now serve as essential tools which improve both predictive risk assessment capabilities and real-time threat monitoring systems. The technological layer enables organizations to assess cybersecurity threats which they can track and document throughout the ERM process for decision-making purposes. The layer functions effectively when its technological elements match organizational operational frameworks and governance models since organizations need these elements to achieve successful technological integration.

The organizational layer functions as the core element of the framework since it establishes the degree to which organizations will maintain their integration capabilities. The layer includes governance structures and risk culture and leadership support. Effective governance mechanisms create structural frameworks which enable organizations to incorporate cybersecurity practices into their ERM processes through board oversight and risk management committees and internal audit functions. Leadership support establishes cybersecurity as a priority strategic risk domain while risk culture establishes a system which ensures people understand their responsibilities for risk management. The study's findings show that this organizational layer functions as the primary element which determines how well organizations achieve their integration goals through its role in implementing regulatory requirements and technological capabilities.

The core framework center point establishes an integration mechanism which uses a central ERM system to integrate cybersecurity risk assessment into enterprise decision-making processes. The mechanism enables organizations to create cybersecurity metrics which align with their main risk indicators thus improving their ability to identify resource needs and upcoming security threats. The integration mechanism establishes continuous system monitoring with feedback functions which ensure system compliance with changing regulatory standards and emerging threat patterns.

The framework produces three main benefits which include improved organizational resilience and better regulatory compliance as well as increased visibility into potential risks. The framework enables financial institutions to create unified cybersecurity programs by linking regulatory requirements with their existing technological resources and organizational capabilities. The Nigerian financial system needs a complete model which considers all aspects of its complex financial system.



ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 4 Context-Aware Framework for Cybersecurity–ERM Integration in Nigeria's Financial Industry

The figure can be conceptualized as a concentric, multi-layered model. The outer layer displays the regulatory framework which includes CBN requirements, NDIC requirements, and NDPR requirements. The middle layer displays technological capabilities which include IT infrastructure and cybersecurity tools and data analytics capabilities. The inner layer displays organizational elements which include governance structures and cultural values and leadership practices. The central ERM integration mechanism connects all layers through its hub-based system which directs cybersecurity risk assessment into enterprise decision-making processes. The bidirectional arrows between the layers show that the layers maintain ongoing interaction which results in feedback while showing that integration functions as an evolving process which requires multiple implementation steps.

For further clarity, Table 2 summarizes the key components of each layer and their roles within the framework.

Table 2 Summary of Framework Components and Roles

Layer	Key Components	Role in Integration
Regulatory	CBN, NDIC, NDPR	Drives adoption through compliance and oversight
Technological	IT infrastructure, cybersecurity tools, data analytics	Enables implementation and real-time risk monitoring
Organizational	Governance, risk culture, leadership	Drives internalization and sustainability of integration
Integration Mechanism	Central ERM system	Aligns cybersecurity with enterprise risk decision-making

Implications

The research results together with the developed framework provide theoretical and practical outcomes which support the progress of cybersecurity knowledge and practice in financial systems of emerging economies through their ERM integration process.

Theoretical Implications

The research extends the Technology–Organization–Environment (TOE) framework through its application to cybersecurity–ERM integration which represents a more intricate and presently uninvestigated field of study. The research shows how TOE applies to organizational processes which beyond initial adoption, include risk internalization and strategic alignment and governance integration (Tornatzky & Fleischer, 1990). The study extends its analytical framework through the inclusion of institutional theory which demonstrates how regulatory forces drive adoption while simultaneously dictating the integration degree and adoption intensity. The study establishes cybersecurity as a fundamental risk domain which organizations need to manage because it exists beyond the range of standard IT risk management activities. The new definition of risks establishes a connection which matches current risk management practices which deal with operational and technological and strategic risks as interconnected systems (Biener et al., 2015). The new context-aware framework establishes a multi-layered framework which shows how external pressures and internal capabilities interact to create a comprehensive model for studying cybersecurity–ERM integration.

Practical Implications

The study provides Nigerian financial institutions with practical guidance through its research outcomes. The framework functions as a strategic tool which organizations need to achieve their cybersecurity and enterprise risk management objectives. The study demonstrates that organizations need to implement active risk management solutions which go beyond basic compliance requirements. The framework enables financial institutions to evaluate their current maturity level across three domains which include regulatory compliance and technological capabilities and organizational development while it helps them detect integration obstacles. The findings demonstrate to regulators and policymakers that they must create policies, which both enforce compliance and enable institutional capacity development. The Central Bank of Nigeria (CBN) and the National Information Technology Development Agency (NITDA) should use these insights to create frameworks which improve organizational cybersecurity integration into their enterprise risk management systems. The study shows that regulators must work together with industry stakeholders to create regulatory requirements which will function properly in combination with upcoming technological developments.

Limitations and Future Research

The study presents several limitations which need recognition because they define research boundaries which help understand study outcomes and create research pathways to follow. The main restriction prevents research from creating targets because its theoretical framework defines all of its study parameters. The study depends on literature synthesis and theoretical reasoning because it lacks empirical data to validate its findings. The framework development process requires this method but it creates restrictions which stop researchers from applying their results to different situations and finding direct connections between the identified factors and cybersecurity–ERM integration results. The proposed framework functions as a conceptual model which needs scientific validation through real-world testing. The study exists within a limited geographical area which only includes the Nigerian financial sector as its complete research territory. Nigeria serves as an excellent study location because its financial system develops rapidly while its regulatory framework evolves, but researchers should not apply findings from this study to other countries which have dissimilar institutional frameworks and technological systems and cultural patterns. The framework will not work for all countries because different nations apply regulatory systems and their technological systems have different levels of development and their organizations follow distinct operational methods.

Future Research Directions

The research team needs to conduct framework testing through real-world implementation because that process will handle existing research obstacles. Researchers can use quantitative methods through surveys and structural equation modeling to examine how regulatory and technological and organizational elements influence cybersecurity-ERM integration. The studies will produce statistical data which proves or enhances the existing conceptual framework. The research team will study how different financial institutions, including commercial banks and microfinance institutions and fintech firms, integrate their systems because that process creates diverse organizational patterns. The research team will conduct cross-country studies which include regions outside Nigeria to identify

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

global study results which can lead to the creation of universal study models. Researchers should examine how artificial intelligence and blockchain technology affect cybersecurity-ERM integration because these technologies are becoming essential in our modern digital environment.

CONCLUSION

The practice of linking cybersecurity with Enterprise Risk Management (ERM) systems operates as an essential requirement to protect financial systems from disturbances while maintaining their ability to operate normally in developing nations like Nigeria. Financial institutions face rising digital security challenges because they depend on digital systems which create more frequent and complex cyber threats, requiring them to adopt risk management solutions that cover all aspects of their operations. The research investigates the factors that determine how organizations implement cybersecurity measures according to their Enterprise Risk Management systems by using the Technology–Organization–Environment framework together with institutional theory. The study demonstrates that organizations successfully achieve their integration goals through three essential elements which include compliance with regulatory standards and the implementation of technological systems and their organizational capacity. Regulatory pressures play a crucial role in initiating adoption but they create obstacles which prevent organizations from achieving complete system integration. The organization can achieve implementation through its technological systems but their performance depends on their compatibility with the organization. The organization factors which include governance structures and leadership commitment and risk culture create the strongest effect on organizations which want to achieve enduring integration. The study introduces a context-aware framework which shows how regulatory and technological and organizational elements interact with each other through an ERM system that functions as the central point of integration. The framework offers organizations a systematic way to integrate cybersecurity risks into their enterprise decision-making which boosts risk visibility and compliance and organizational capacity to handle challenges.

REFERENCES

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research, 9*(2), 204–215.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003.

Basel Committee on Banking Supervision. (2011). *Principles for the sound management of operational risk*. Bank for International Settlements.

Basel Committee on Banking Supervision. (2018). *Cyber-resilience: Range of practices*. Bank for International Settlements.

Behl, A., Jayawardena, N., Pereira, V., & Islam, N. (2022). Cybersecurity and cyberwar: What everyone needs to know. *Journal of Business Research, 144*, 113–122.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance—Issues and Practice, 40*(1), 131–158.

Central Bank of Nigeria. (2018). *Risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers*. CBN.

Central Bank of Nigeria. (2022). *Guidelines on information security standards*. CBN.

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. *Information Management & Computer Security, 17*(1), 4–15.

COSO. (2017). *Enterprise risk management: Integrating with strategy and performance*. Committee of Sponsoring Organizations of the Treadway Commission.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160.

ENISA. (2021). *Cybersecurity and resilience of smart financial ecosystems*. European Union Agency for Cybersecurity.

EY. (2021). *Global information security survey*. Ernst & Young.

Gartner. (2020). *Top security and risk management trends*. Gartner Research.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33–56.

ISO. (2018). *ISO 31000: Risk management—Guidelines*. International Organization for Standardization.

ISO/IEC. (2022). *ISO/IEC 27001: Information security management systems—Requirements*. International Organization for Standardization.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139–154.

KPMG. (2020). *Cybersecurity considerations in enterprise risk management*. KPMG International.

National Information Technology Development Agency. (2019). *Nigeria Data Protection Regulation (NDPR)*. NITDA.

Nigeria Deposit Insurance Corporation. (2021). *Annual report and statement of accounts*. NDIC.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999116
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

NIST. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology.

NIST. (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. National Institute of Standards and Technology.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation, 14*(1), 110–121.

Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Auerbach Publications.

PwC. (2022). *Global digital trust insights survey*. PricewaterhouseCoopers.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems*. NIST.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

World Bank. (2021). *Cybersecurity in financial sector development*. World Bank Group.

Zhang, P., & Li, N. (2019). The importance of cybersecurity risk management in financial institutions. *Journal of Financial Regulation and Compliance, 27*(2), 123–137.