ISSN: 6739 - 7466
Volume 10, Number 1, 2026
Journal of Management, Marketing, and Accounting Innovations

Berlin International University of Applied Science, Salzufer 6, 10587 Berlin, Germany
Journal Homepage:www.bwjournal.org
Bushwealth Academic Journals

INFORMATION SECURITY STRATEGY AND ADMINISTRATIVE RISK MANAGEMENT IN TERTIARY INSTITUTIONS IN RIVERS STATE, NIGERIA

ORISAH-GODFREY, Lillian Anyanagba, PhD
lillian.orisah-godfrey@ust.edu.ng
Department of Office and Information Management, Faculty of Administration and Management, Rivers State University, Port Harcourt, Rivers State, Nigeria

GBAFAH, Beauty Lemabari, PhD
beauty.gbafah@rsu.edu.ng
Department of Office and Information Management, Faculty of Administration and Management, Rivers State University, Port Harcourt, Rivers State, Nigeria

ABSTRACT

This study examined information security strategy and administrative risk management in tertiary institutions in Rivers State, Nigeria. Anchored on the Information Security Management (ISM) Theory and the Enterprise Risk Management (ERM) Framework, the study adopted a correlational survey research design. The predictor variable, information security strategy, was operationalized along two dimensions: cybersecurity policy implementation and data access control mechanisms. The criterion variable, administrative risk management, was measured by risk identification efficiency and risk mitigation effectiveness. The population comprised 428 administrative officers drawn from five selected public tertiary institutions in Rivers State, from which a sample of 204 respondents was determined using Taro Yamane's formula and selected through stratified random sampling. A structured questionnaire with a Cronbach alpha reliability coefficient of 0.87 was employed for data collection. Pearson's Product Moment Correlation Coefficient and simple linear regression, at 0.05 level of significance, were used to test the null hypotheses. Results revealed that information security strategy had a significant positive relationship with risk identification efficiency ($r = .641$, $p < .05$) and risk mitigation effectiveness ($r = .618$, $p < .05$). The study concludes that information security strategy is a significant positive predictor of administrative risk management outcomes in tertiary institutions in Rivers State, Nigeria. It was recommended that tertiary institutions should institutionalise comprehensive cybersecurity policies and strengthen data access control protocols to enhance their administrative risk management capacity.

Keywords: Information Security Strategy, Cybersecurity Policy Implementation, Data Access Control Mechanisms, Administrative Risk Management, Risk Identification Efficiency, Risk Mitigation Effectiveness, Tertiary Institutions

INTRODUCTION

The governance of information assets in public tertiary institutions has emerged as one of the most consequential administrative challenges of the contemporary era. As universities, polytechnics, and colleges of education across Nigeria increasingly depend on digitally enabled administrative systems for student data management, financial operations, personnel records, and institutional communications, these institutions have simultaneously become targets of a growing spectrum of information security threats (Eze & Nkemdirim, 2020; Orisah-Godfrey & Alikornwo, 2026). In Rivers State, Nigeria, where the tertiary education ecosystem includes major public institutions such as the Rivers State University, Ignatius Ajuru University of Education, and Captain Elechi Amadi Polytechnic, the inadequacy of institutional information security governance has manifested in

recurring incidents of unauthorized data access, administrative record manipulation, and digital system vulnerabilities (Alikornwo, Adiele, & Onyebuenyi, 2026; Gbafah, 2026). These developments have exposed the administrative structures of these institutions to material risks that undermine service delivery, compromise stakeholder trust, and jeopardize the integrity of institutional records. Scholars have consistently argued that the formulation and implementation of deliberate information security strategies constitute a foundational governance imperative for any institution that seeks to manage information-related risks effectively (ISO/IEC 27001:2013; Whitman & Mattord, 2018). The growing body of evidence on cybersecurity governance in Nigeria underscores the urgency of this imperative, particularly in the public sector, where policy enforcement gaps and resource constraints create fertile conditions for security breaches (Ikuero, 2022; Federal Ministry of Communications and Digital Economy, 2024).

Administrative risk management, in the context of tertiary education, refers to the structured organizational process through which institutions identify, assess, prioritize, and respond to threats that endanger their administrative operations, data integrity, and institutional accountability (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017; ISO 31000:2018). The increasing digitization of administrative functions has significantly expanded the risk landscape confronting tertiary institutions, introducing information security risks as a dominant category of operational threat. Studies conducted in Nigeria and broader sub-Saharan Africa have documented that tertiary institutions remain structurally ill-equipped to manage these risks, citing factors including the absence of formal risk management frameworks, weak cybersecurity governance, low digital literacy among administrative personnel, and poor alignment between institutional policy and practice (Eze & Chukwu, 2021; Olufowobi, Ogunlade, & Bello, 2019; Justice-Amadi, 2023). In Rivers State specifically, studies by Alikornwo et al. (2026), Orisah-Godfrey and Alikornwo (2026), and Gbafah (2026) have documented persistent deficits in digital governance, information management culture, and administrative security practice within public institutions, establishing a clear empirical context for the present investigation. The absence of a documented, operationally grounded information security strategy in most of these institutions has left their administrative risk management frameworks fragile and reactive, rather than anticipatory and systemic.

A growing number of international scholars have examined information security strategy through multiple theoretical and empirical lenses. Key dimensions that have attracted scholarly attention include cybersecurity policy implementation, data access control mechanisms, security awareness training, incident response procedures, and information asset classification (ISO/IEC 27001:2013; NITDA, 2020; Ukwandu et al., 2023; Whitman & Mattord, 2018). In the Nigerian context, scholars such as Ikuero (2022), Enofogha (2023), and Nte, Enoke, and Omolara (2022) have documented critical gaps in cybersecurity governance, particularly in the public sector, demonstrating that policy intentions rarely translate into operational outcomes due to structural, capacity, and funding deficiencies. These gaps are especially pronounced in tertiary institutions where administrative risk management functions are frequently delegated to personnel with limited information security competence (Alikornwo et al., 2026; Kalagbor & Adiele, 2026; Adiele & Sam-Kalagbor, 2026). The theoretical framework of this study draws on the Information Security Management Theory, which integrates technical, organizational, and human behavioral dimensions of security governance (Siponen & Willison, 2009), and the Enterprise Risk Management Framework, which provides a holistic model for understanding how institutions identify, assess, and mitigate operational risks (COSO, 2017). Together, these frameworks provide a robust conceptual foundation for empirically investigating the relationship between information security strategy and administrative risk management in the study context.

Regardless of the growing body of literature on information security and institutional management in Nigeria, there remains a conspicuous scarcity of empirical studies that specifically examine how information security strategy, as an integrated institutional construct, predicts administrative risk management outcomes in Rivers State tertiary institutions. Most extant studies have either focused on technical cybersecurity issues at the national level (Ikuero, 2022; Enofogha, 2023) or have examined administrative performance outcomes without specifically addressing information security strategy as a predictor variable (Justice-Amadi, 2023; Alikornwo & Nwinyokpugi, 2025; Alikornwo & Adiele, 2024). The present study was therefore designed to fill this gap by providing empirical evidence on the relationship between information security strategy and administrative risk management, operationalized as risk identification efficiency and risk mitigation effectiveness, in tertiary institutions in Rivers State, Nigeria. The significance of the study lies in its potential to provide evidence-based guidance for institutional administrators, policymakers, and scholars on the role of information security governance in strengthening administrative risk management capacity in the Nigerian tertiary education sector.

Statement of the Problem

Tertiary institutions in Rivers State continue to grapple with an escalating array of information security risks that directly compromise administrative risk management effectiveness. Administrative personnel in these institutions routinely handle sensitive data including student academic records, staff personnel files, financial statements, examination materials, and institutional correspondence, often without the protection of formally instituted information security strategies or risk management protocols (Alikornwo et al., 2026; Orisah-Godfrey & Alikornwo, 2026; Gbafah, 2026). Incidents of unauthorized access to institutional databases, deliberate manipulation of academic records, loss of administrative data during system failures, and exploitation of weak data access control systems have been documented across public tertiary institutions in the South-South geopolitical zone of Nigeria, with Rivers State institutions being particularly vulnerable given the high volume of administrative data they generate and process (Eze & Nkemdirim, 2020; Eze & Chukwu, 2021). These challenges are compounded by the absence of formalised information security policies in most of these institutions, the lack of dedicated information security governance units, and the dearth of structured risk identification and mitigation protocols within administrative departments. While scholars have examined various dimensions of digital governance, administrative performance, and institutional management in Rivers State, the specific empirical relationship between information security strategy and administrative risk management outcomes has not been systematically investigated. This constitutes the critical research gap that the present study addresses, with the aim of generating empirical evidence that can inform institutional policy and administrative practice in Rivers State tertiary institutions.

LITERATURE REVIEW

Conceptual Review

Information Security Strategy

Information security strategy refers to the comprehensive, deliberate, and institutionally anchored set of policies, procedures, technical controls, and governance mechanisms that an organization deploys to protect its information assets from unauthorized access, disclosure, alteration, destruction, and disruption (ISO/IEC 27001:2013; Whitman & Mattord, 2018). It encompasses both the formulation and operationalisation of security objectives, spanning the full lifecycle of institutional data from creation and storage to transmission, use, and disposal. In the context of tertiary institutions, information security strategy governs the protection of academic records,

financial data, personnel information, examination materials, research outputs, and all other categories of institutionally sensitive data that, if compromised, could cause significant harm to institutional operations, stakeholder welfare, and public trust (Eze & Nkemdirim, 2020; Orisah-Godfrey & Alikornwo, 2026). A functionally effective information security strategy integrates technical solutions with organizational governance structures, ensuring that the human, policy, and technological dimensions of information security are coherently aligned (Siponen & Willison, 2009; Whitman & Mattord, 2018). According to ISO/IEC 27001:2013, the international standard for information security management systems, effective strategy implementation requires visible top management commitment, a systematic approach to risk assessment, and the deployment of context-appropriate security controls across all organizational processes.

In the Nigerian tertiary education environment, information security strategy has historically been underdeveloped, fragmented, and largely reactive, with most institutions relying on generic IT usage guidelines or informal security practices rather than formally documented and enforced security frameworks (Eze & Chukwu, 2021; Olufowobi, Ogunlade, & Bello, 2019; Federal Ministry of Communications and Digital Economy, 2024). Alikornwo et al. (2026) demonstrated that in Rivers State government MDAs, strategic information management deficits, including the absence of data security protocols and the inadequacy of records automation systems, significantly undermined administrative productivity and information accessibility. Orisah-Godfrey and Alikornwo (2026) similarly found that information governance strategy, particularly in the dimensions of process automation and data integration, had a significant positive relationship with administrative accountability in public sector institutions in Rivers State, a finding that underscores the broad strategic importance of information governance for institutional performance outcomes. For the purposes of the present study, information security strategy is operationalized through two principal dimensions: cybersecurity policy implementation and data access control mechanisms.

Cybersecurity Policy Implementation

Cybersecurity policy implementation refers to the practical operationalisation of documented cybersecurity policies, standards, and guidelines within an organization, translating policy intentions into specific behaviors, technical controls, and institutional procedures that govern how personnel interact with digital systems and information assets (Adeleke & Oladipupo, 2023; Ikuero, 2022). Effective cybersecurity policy implementation encompasses the enforcement of password management protocols, regular staff training on digital threats and security responsibilities, the establishment of incident reporting channels, the periodic auditing of information systems for vulnerabilities, and the systematic monitoring of user compliance with security standards (ISO/IEC 27001:2013; NITDA, 2020). Mbanaso et al. (2022) argued that the effectiveness of cybersecurity policy implementation in Nigerian public institutions is consistently constrained by weak inter-agency coordination, inadequate technical expertise, and outdated ICT infrastructure, challenges that are directly mirrored in the tertiary education sector.

At the institutional level, cybersecurity policy implementation determines the extent to which administrative personnel understand and comply with information security obligations, the adequacy of institutional responses to security incidents, and the degree to which security governance is embedded in routine administrative practice (Nte, Enoke, & Omolara, 2022; Federal Ministry of Communications and Digital Economy, 2024). Ikuero (2022) found that the National Cybersecurity Policy and Strategy of Nigeria, while providing a nationally applicable framework, has limited operational reach in public institutions due to poor enforcement, capacity deficits, and the absence of institution-level cybersecurity governance structures. Eze and Chukwu (2021) corroborated this finding in their assessment of Nigerian public universities, demonstrating that most institutions

lacked formalized cybersecurity policies, trained security personnel, and incident response procedures. These structural gaps in cybersecurity policy implementation create significant vulnerabilities that directly impair the administrative risk management capacity of tertiary institutions.

Data Access Control Mechanisms

Data access control mechanisms refer to the technical and administrative measures employed by an organization to restrict access to its information assets to authorised personnel only, preventing unauthorized disclosure, modification, or destruction of data (ISO/IEC 27001:2013; Jacobson & Idziorek, 2013). These mechanisms include user authentication systems such as passwords, biometric devices, and multi-factor authentication; role-based access control frameworks that calibrate data access privileges according to job function and authorization level; audit trails and access logs that provide an accountable record of all interactions with sensitive institutional data; and physical access controls such as biometric door locks and restricted server room access (NITDA, 2020; Ukwandu et al., 2023). In educational institutions, the diversity and volume of data users, encompassing students, administrative staff, academic staff, and external stakeholders, make data access control particularly complex and critical.

Empirical evidence from Nigeria consistently identifies data access control weaknesses as a primary driver of information security breaches in public institutions. Alikornwo et al. (2026) found that Rivers State government MDAs frequently failed to implement adequate access control protocols, resulting in exposure of administrative data to unauthorized users and compromising data security. The Federal Ministry of Communications and Digital Economy (2024) similarly identified inadequate access control systems, including the widespread use of shared and generic login credentials, as key contributors to the high incidence of data breaches in Nigerian public institutions. Gbafah (2026) demonstrated that digital literacy deficits among administrative staff in Rivers State tertiary institutions significantly limited their ability to apply available access control tools effectively, creating persistent security vulnerabilities even in institutions that had nominally invested in digital security infrastructure. These findings collectively underscore the centrality of data access control mechanisms in any comprehensive information security strategy for tertiary institutions.

Administrative Risk Management

Administrative risk management refers to the systematic, proactive, and institutionally embedded process through which organizations identify, assess, prioritize, monitor, and respond to risks that threaten their administrative efficiency, institutional integrity, and service delivery capacity (COSO, 2017; ISO 31000:2018). In the tertiary education context, administrative risk management encompasses the full range of activities through which institutional administrators anticipate and address threats to academic records, financial systems, personnel management, physical infrastructure, and information systems (Okwu, Tantua, & Obara, 2023; Justice-Amadi, 2023). The growing digitization of administrative functions in Nigerian tertiary institutions has substantially expanded the risk landscape, introducing information security risks as a dominant and increasingly complex category of operational threat that demands deliberate managerial attention (Alikornwo et al., 2026; Kalagbor & Adiele, 2026). COSO (2017) posits that effective enterprise risk management is distinguished by the integration of risk management functions into the organization's overall governance architecture, ensuring that risk identification, assessment, and response mechanisms are systematically embedded in institutional operations rather than activated only in response to crises.

In Rivers State tertiary institutions, administrative risk management has been shaped by a complex interplay of resource constraints, institutional culture, policy gaps, and governance capacity limitations. Alikornwo et al. (2026) demonstrated that in Rivers State government MDAs, persistent deficits in strategic information management led to heightened exposure to administrative risks, including data loss, unauthorized record alteration, and service delivery failures. Adiele and Sam-Kalagbor (2026) similarly found that the effectiveness of administrative decision-making in Rivers State local government councils was significantly mediated by the quality of information management systems, suggesting that risk-informed governance is conditional on the adequacy of institutional information practices. Alikornwo, Sam-Kalagbor, and Nyeche (2026) established that administrative strategy, particularly its dimensions of process automation and data integration, significantly predicted institutional efficiency and responsiveness in Rivers State public institutions, providing empirical grounding for the contention that strategic approaches to information management underpin effective risk governance. For the purposes of the present study, administrative risk management is measured by two dimensions: risk identification efficiency and risk mitigation effectiveness.

Risk Identification Efficiency

Risk identification efficiency refers to the organizational capacity to detect, document, and escalate threats to institutional information assets and administrative processes accurately, comprehensively, and promptly (ISO 31000:2018; COSO, 2017). It encompasses the quality of institutional risk sensing mechanisms, the robustness of threat monitoring and reporting systems, the clarity of risk communication channels, and the speed with which identified risks are escalated to appropriate management levels (Whitman & Mattord, 2018; Federal Ministry of Communications and Digital Economy, 2024). In the administrative context of tertiary institutions, risk identification efficiency reflects the degree to which administrative personnel recognize and report information security incidents, the extent to which risk identification is institutionalized through formal procedures, and the availability and utilisation of adequate tools for monitoring institutional information systems for anomalous activities (Eze & Nkemdirim, 2020; Eze & Chukwu, 2021).

The empirical literature documents pervasive deficits in risk identification efficiency in Nigerian public tertiary institutions. Eze and Chukwu (2021) found that most Nigerian public universities become aware of information security risks only after incidents have materially affected institutional operations, indicating a culture of reactive rather than proactive risk identification. Orisah-Godfrey and Alikornwo (2026) observed that in Rivers State public sector institutions, administrative personnel demonstrated low levels of risk awareness and reporting behavior, with risk identification activities largely confined to post-incident reviews rather than systematic, continuous monitoring. The absence of dedicated risk management units, the lack of structured risk identification training for administrative staff, and the unavailability of appropriate monitoring tools collectively constrain risk identification efficiency in these institutions. These findings underscore the need for strategic interventions, particularly through information security policy frameworks, that can embed risk identification as a routine component of administrative governance.

Risk Mitigation Effectiveness

Risk mitigation effectiveness refers to the degree to which an organization successfully reduces the likelihood, severity, and organizational impact of identified information security risks through deliberate, resource-supported, and evidence-based interventions (COSO, 2017; ISO 31000:2018). Risk mitigation strategies in the information security domain encompass technical controls including firewalls, encryption, intrusion detection systems, and secure backup mechanisms; administrative

controls including security policy enforcement, access rights reviews, and regular security audits; and human resource controls including security awareness training, disciplinary procedures, and background verification for personnel with access to sensitive data (ISO/IEC 27001:2013; Whitman & Mattord, 2018). The effectiveness of these measures is determined not only by their technical sophistication but also by the organizational culture, management commitment, and resource allocation that sustain them over time (Adeyemi & Oluwaseun, 2024; Mbanaso et al., 2022).

In the Nigerian context, risk mitigation effectiveness in tertiary institutions has been widely found to be inadequate. Eze and Chukwu (2021) found that fewer than a third of surveyed Nigerian public universities had documented risk mitigation plans or incident response procedures, highlighting a critical gap in institutional risk governance. Alikornwo et al. (2026) documented that even where digital security technologies existed in Rivers State government institutions, risk mitigation effectiveness was severely constrained by inadequate personnel training, poor maintenance of security systems, and the absence of dedicated budget allocations for information security management. Gbafah (2026) established that digital literacy limitations among administrative staff significantly impaired their capacity to deploy available risk mitigation tools, resulting in persistent vulnerabilities even in institutions that had nominally invested in security infrastructure. These findings collectively establish risk mitigation effectiveness as a multi-dimensional construct that is sensitive to the quality of information security strategy, the competence of administrative personnel, and the adequacy of institutional governance structures.

Theoretical Framework

Information Security Management Theory

The Information Security Management (ISM) Theory provides a foundational explanatory framework for understanding how organizations establish, implement, maintain, and continuously improve their information security practices (Siponen & Willison, 2009; Whitman & Mattord, 2018). The theory holds that effective information security management is the product of the coherent integration of three interacting dimensions: technical controls, which encompass the hardware and software mechanisms deployed to protect information systems; organizational controls, which include the policies, procedures, and governance structures that guide security behavior; and human behavioral controls, which reflect the security awareness, competency, and compliance of system users. This tripartite integration is central to the theory's explanatory power, as it recognizes that technological investments in information security yield diminishing returns in the absence of corresponding policy frameworks and behavioral compliance among personnel. ISM Theory thus provides a holistic lens through which the relationship between institutional information security strategy and organizational outcomes can be analyzed.

The relevance of ISM Theory to the present study is direct and multidimensional. The theory predicts that institutions with well-formulated and robustly implemented information security strategies, encompassing both cybersecurity policies and data access control mechanisms, will demonstrate superior risk management outcomes compared to institutions with weak or absent security governance frameworks. This prediction is consistent with the findings of Eze and Chukwu (2021), Orisah-Godfrey and Alikornwo (2026), and the Federal Ministry of Communications and Digital Economy (2024), all of which document that policy and control deficits in information security governance are significantly associated with poor institutional risk management outcomes in the Nigerian public sector. ISM Theory also highlights the critical role of organizational commitment to security governance, arguing that the mere existence of policy documents without enforcement, training, and resource support will fail to produce the desired risk management outcomes. This theoretical insight is particularly relevant in the Rivers State context, where the gap between policy

formulation and operational implementation in information security governance has been extensively documented.

Enterprise Risk Management Framework

The Enterprise Risk Management (ERM) Framework, as developed and periodically updated by the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2017), provides a comprehensive, integrated approach to organizational risk management that has been widely adopted in both public and private sector organizations globally. The ERM Framework is predicated on the premise that risk management is most effective when it is woven into the strategic and operational fabric of the organization, rather than being treated as a reactive, compliance-driven function. According to COSO (2017), effective ERM encompasses five interconnected components: governance and culture; strategy and objective-setting; performance; review and revision; and information, communication, and reporting. Each component makes a distinct contribution to the organization's overall capacity to manage risks in alignment with its strategic objectives and stakeholder expectations. The framework's emphasis on information and communication as enabling infrastructure for effective risk governance provides a direct theoretical bridge to the present study's investigation of information security strategy as a predictor of administrative risk management outcomes.

The application of the ERM Framework to this study is grounded in its operationalization of risk identification and risk mitigation as measurable, institutionally determined governance outcomes. The framework argues that organizations which invest in robust information governance, including information security controls, access management systems, and cybersecurity policies, are simultaneously strengthening the information and communication infrastructure that sustains effective risk identification and mitigation across the organization. This theoretical position aligns directly with the present study's hypotheses and is further supported by ISO 31000:2018, which emphasizes the iterative nature of risk management and the importance of continual improvement in risk governance processes. The coherence between ISM Theory and the ERM Framework reinforces the conceptual integrity of the study's framework and provides a theoretically grounded basis for predicting a significant positive relationship between information security strategy and administrative risk management in Rivers State tertiary institutions.

Empirical Review

Orisah-Godfrey and Alikornwo (2026) investigated information governance strategy and administrative accountability referents in public sector institutions in Rivers State, Nigeria, operationalizing information governance strategy through process automation and data integration as predictor variable, and administrative accountability as criterion variable. The study demonstrated that information governance strategy had a significant and positive relationship with administrative accountability, establishing that strategic information management frameworks are critical drivers of institutional accountability outcomes in the Rivers State public sector context. This study is directly relevant to the present investigation as it establishes the predictive power of information governance strategy, a construct closely related to information security strategy, for institutional administrative outcomes in the same geopolitical environment.

Alikornwo et al. (2026) empirically examined information management in digitally enabled offices, evaluating administrative productivity in Rivers State government MDAs. Using records automation and digital filing systems as dimensions of digital office administration, and measuring information management success through information accessibility and data security, the study found significant positive relationships between records automation and information accessibility (r = .652) and data

security (r = .590), using Pearson's Product-Moment Correlation and a correlational survey design with 112 administrative and ICT personnel. The study concluded that strategic investment in digital office technologies and personnel training is essential for securing administrative data and enhancing service delivery. This empirical evidence directly informs the present study's conceptualisation of data security as a measurable dimension of administrative risk management.

Alikornwo, Adiele, and Dornanu (2025) examined digital transformation as a corollary for administrative decision-making in government ministries in Rivers State. The study demonstrated that dimensions of digital transformation, particularly those related to information digitization and administrative process redesign, significantly predicted decision-making quality and timeliness in government ministries. These findings reinforce the present study's theoretical position that strategic information management initiatives, including information security frameworks, have significant implications for administrative governance outcomes in Rivers State public institutions.

Kalagbor and Adiele (2026) investigated e-governance and democratic accountability, assessing the information management capacity of the public sector in Rivers State, Nigeria. Anchored on information governance theory, the study examined the relationship between e-governance adoption, information management capacity, and democratic accountability, finding significant relationships among these constructs. The study noted that persistent bureaucratic delays and forms of administrative vulnerability arising from limited information governance capacity significantly undermined accountability outcomes. This study is relevant to the present investigation as it establishes the institutional context of information governance deficits in the same geopolitical environment and provides empirical evidence for the relationship between information management capacity and administrative governance quality.

Adiele and Sam-Kalagbor (2026) examined bureaucratic decision-making and the leveraging of strategic information use in local government councils in Rivers State. The study found that dimensions of strategic information use, specifically data integration and information-seeking behavior, significantly predicted decision timeliness and accuracy across the 23 Local Government Areas of Rivers State. These results underscore the critical mediating role of robust information management systems in administrative processes and provide empirical support for the present study's argument that information security strategy, as a component of strategic information management, is a significant predictor of administrative risk management outcomes.

Alikornwo et al. (2026b) empirically examined administrative strategy and public sector effectiveness through a digital information management triangulation in Rivers State. The study demonstrated that administrative strategy significantly predicted institutional efficiency (R2 = .617) and responsiveness (R2 = .491), with digital information management systems exerting a substantial mediating effect accounting for 56.6 percent of the variance in the strategy-performance relationship. This finding underscores the centrality of digital information governance, including its security dimensions, as a mediating mechanism between strategic intent and institutional performance.

Orisah-Godfrey (2026) examined the relationship between leadership communication strategy and administrative staff commitment in educational institutions in Rivers State, Nigeria, using a correlational survey design with 238 administrative staff. The study found a significant positive relationship between leadership communication strategy and administrative staff commitment, with job satisfaction as a significant mediating variable. While this study addressed communication and commitment rather than information security directly, its findings regarding the governance structures and administrative challenges facing tertiary institutions in Rivers State provide important contextual grounding for the present investigation.

Okwu et al. (2023) examined enterprise alignment adoption strategies and quality healthcare in South-South Nigeria, establishing a significant relationship between information systems alignment and institutional service quality. This study provides cross-sectoral empirical evidence for the relationship between information governance strategy and institutional performance outcomes in the South-South Nigerian context.

Justice-Amadi (2023) examined change management and job performance of office managers in tertiary institutions in Rivers State, finding that technological change management had the strongest positive effect on office managers' performance. This finding is relevant to the present study as it establishes that the manner in which institutions manage digital and technological transitions, a dimension closely related to cybersecurity policy implementation, significantly influences administrative performance outcomes in Rivers State tertiary institutions. A companion study by Justice-Amadi (2023) on organizational citizenship behaviour of office managers in the same institutional context reinforced the importance of behavioral and organizational factors in determining administrative effectiveness.

Eze and Nkemdirim (2020) investigated the management of information security in public universities in Nigeria through a literature-based analysis. The study identified common threats to information security in Nigerian higher education institutions and documented the critical absence of formalized security policies, trained security personnel, and adequate incident response procedures in most public universities. The study's findings provide empirical grounding for the present investigation's identification of cybersecurity policy implementation and data access control mechanisms as critical governance gaps in Nigerian tertiary institutions.

Eze and Chukwu (2021) conducted an empirical assessment of information security risk in Nigerian public universities. Their findings, that fewer than a third of surveyed institutions had documented risk mitigation plans, incident response procedures, or business continuity arrangements, directly inform the present study's operationalization of risk identification efficiency and risk mitigation effectiveness as measurable dimensions of administrative risk management performance. The study highlighted the urgent need for institutional frameworks that systematically embed risk identification and mitigation functions within the administrative governance of Nigerian tertiary institutions.

Olufowobi, Ogunlade, and Bello (2019) examined cybersecurity practices in Nigerian higher institutions and demonstrated that while institutional awareness of cybersecurity threats had improved, the translation of awareness into practice remained constrained by resource shortfalls, policy enforcement gaps, and the absence of dedicated information security governance structures. These findings reinforce the present study's theoretical premise that effective information security strategy requires not only policy formulation but also structural and resource commitments from institutional management.

Mbanaso et al. (2022) analyzed cybersecurity governance challenges in Nigeria, identifying insider threats, phishing attacks, and weak access control protocols as the most prevalent information security risks confronting Nigerian public institutions. Their recommendations for comprehensive information security strategy development in public institutions are directly aligned with the present study's research focus and theoretical framework.

Ikuero (2022) conducted a critical review of cybersecurity governance in Nigeria, identifying substantial policy-enforcement challenges within governmental institutions. The study demonstrated that the National Cybersecurity Policy and Strategy, despite its structural comprehensiveness, had limited operational reach in public institutions due to insufficient inter-agency collaboration, technical capacity deficits, and outdated ICT infrastructure. The study's contextual findings provide important national-level framing for the present study's institutional-level investigation of cybersecurity policy implementation in Rivers State tertiary institutions.

Nte et al. (2022) evaluated the challenges of mainstreaming cybersecurity laws and privacy protection in Nigeria, demonstrating that while the Cybercrimes Act of 2015 provides a foundational legal framework, its practical implementation at the institutional level remains inadequate. Their call for institution-specific cybersecurity policies that operationalize national legal frameworks into actionable procedures is directly aligned with the present study's focus on cybersecurity policy implementation as a dimension of information security strategy.

Enofogha (2023) conducted a comparative analysis of cybersecurity strategies, policies, and measures between Nigeria and other nations, highlighting that Nigeria's cybersecurity policy efforts have been consistently undermined by the absence of a skilled workforce and specialized training institutions. The study's emphasis on capacity building as a prerequisite for effective cybersecurity policy implementation has direct implications for tertiary institution administrators seeking to improve their information security governance and, by extension, their administrative risk management outcomes.

Adeyemi and Oluwaseun (2024) examined the role of human capital in cybersecurity implementation in Nigeria, establishing that organizations with higher investments in cybersecurity training and capacity development reported significantly better cybersecurity performance outcomes. This finding provides empirical support for the present study's multi-dimensional conceptualisation of information security strategy and reinforces the recommendation for sustained human capital investment as a risk management intervention.

Hypotheses

Based on the foregoing empirical review and theoretical framework, the following null hypotheses were formulated and tested at 0.05 level of significance:

H_{01}: There is no significant relationship between information security strategy and risk identification efficiency in tertiary institutions in Rivers State, Nigeria.

H_{02}: There is no significant relationship between information security strategy and risk mitigation effectiveness in tertiary institutions in Rivers State, Nigeria.

METHODOLOGY

This study adopted the correlational survey research design, which is suitable for empirically determining the nature and magnitude of the relationship between variables without manipulating them, thereby allowing the researchers to establish the predictive relationship between information security strategy and administrative risk management as they naturally exist in the study environment. The population of the study comprised 428 administrative officers drawn from five selected public tertiary institutions in Rivers State, Nigeria, namely: Rivers State University, Ignatius Ajuru University of Education, Captain Elechi Amadi Polytechnic, Ken Saro-Wiwa Polytechnic, and Rivers State College of Health Science and Management Technology. The selection of these five institutions was guided by their status as accredited, actively operational public tertiary institutions with substantial administrative staff populations and digitized administrative processes. Using Taro Yamane's (1967) sample size formula at a 5 percent margin of error, n = N / (1 + N(e)2), a sample of 204 respondents was computed from the study population of 428. Stratified random sampling was subsequently applied to allocate respondents proportionately across the five institutions, ensuring equitable representation. Data were collected through a structured, researcher-designed questionnaire titled the "Information Security Strategy and Administrative Risk Management Questionnaire" (ISSARMQ), organized into five sections: the bio-data section and four substantive sections corresponding to the study's four variable dimensions, namely cybersecurity policy implementation, data access control mechanisms, risk identification efficiency, and risk mitigation

effectiveness. All substantive items were measured on a four-point Likert scale anchored at Strongly Agree (4) and Strongly Disagree (1), with a mean threshold of 2.50 used to determine agreement or disagreement on each item. The instrument was validated through face and content validity reviews conducted by three subject specialists in office technology and management, information management, and research methodology, whose suggestions were incorporated into the final instrument. A pilot test conducted with 20 administrative officers from a related institution, the Ignatius Ajuru University of Education Rumuolumeni Campus, yielded a Cronbach alpha reliability coefficient of 0.87, indicating high internal consistency and suitability for the study. Administration of the final instrument was conducted by the researchers and four trained research assistants over a three-week period, and 198 out of 204 copies distributed (97.1 percent) were duly completed and returned, constituting the data set for analysis. Descriptive statistics, specifically mean and standard deviation, were computed for all variable dimensions. For hypothesis testing, Pearson's Product Moment Correlation Coefficient was used to determine the direction and strength of the relationship between the predictor variable, information security strategy, and each measure of the criterion variable, risk identification efficiency and risk mitigation effectiveness. Simple linear regression was further employed to establish the predictive capacity and statistical significance of the observed relationships. All analyses were conducted using IBM SPSS version 25.0 at a 0.05 level of significance.

RESULTS

The results of the hypothesis testing are presented in Tables 1 and 2 below.

Test of Hypothesis One

H01: There is no significant relationship between information security strategy and risk identification efficiency in tertiary institutions in Rivers State, Nigeria.

Table 1: Correlation and Regression of Information Security Strategy on Risk Identification Efficiency

Variables	N	r	r2	Sig.(p)	B	SE	F	df	Decision
Information Security Strategy Risk Identification Efficiency	198	.641	.411	.000	.503	.044	136.74	1, 196	Reject Ho1

The results in Table 1 reveal that information security strategy had a significant positive relationship with risk identification efficiency ($r = .641$, $p = .000 < .05$). The coefficient of determination ($r2 = .411$) indicates that approximately 41.1 percent of the variance in risk identification efficiency was explained by information security strategy. The regression analysis further confirms statistical significance, $F(1, 196) = 136.74$, $p < .05$, with an unstandardized regression coefficient of $B = .503$, indicating that a unit increase in information security strategy is associated with a 0.503 unit increase in risk identification efficiency. On the basis of these findings, the null hypothesis which states that there is no significant relationship between information security strategy and risk identification efficiency in tertiary institutions in Rivers State, Nigeria is rejected at the 0.05 level of significance. The study therefore concludes that information security strategy is a significant positive predictor of risk identification efficiency in the study context.

Test of Hypothesis Two

H02: There is no significant relationship between information security strategy and risk mitigation effectiveness in tertiary institutions in Rivers State, Nigeria.

ISSN: 6739 - 7466
Volume 10, Number 1, 2026
Journal of Management, Marketing, and Accounting Innovations

Berlin International University of Applied Science, Salzufer 6, 10587 Berlin, Germany
Journal Homepage:www.bwjournal.org
Bushwealth Academic Journals

Table 2: Correlation and Regression of Information Security Strategy on Risk Mitigation Effectiveness

Variables	N	r	r2	Sig.(p)	B	SE	F	df	Decision
Information Security Strategy Risk Mitigation Effectiveness	198	.618	.382	.000	.481	.043	121.43	1, 196	Reject Ho2

The results presented in Table 2 show that information security strategy had a significant positive relationship with risk mitigation effectiveness ($r = .618$, $p = .000 < .05$). The coefficient of determination ($r2 = .382$) indicates that approximately 38.2 percent of the variance in risk mitigation effectiveness was accounted for by information security strategy. The regression analysis establishes that the predictive relationship is statistically significant, $F(1, 196) = 121.43$, $p < .05$, with an unstandardized regression coefficient of $B = .481$, indicating that a unit increase in information security strategy is associated with a 0.481 unit increase in risk mitigation effectiveness. The null hypothesis which states that there is no significant relationship between information security strategy and risk mitigation effectiveness in tertiary institutions in Rivers State, Nigeria is accordingly rejected at the 0.05 level of significance. The study therefore concludes that information security strategy is a significant positive predictor of risk mitigation effectiveness in the study context.

Discussion of Findings

The finding from Hypothesis One, establishing a significant positive relationship between information security strategy and risk identification efficiency ($r = .641$, $p < .05$; $r2 = .411$), is consistent with the theoretical predictions of the Information Security Management Theory, which holds that institutions with coherent, well-implemented security governance frameworks develop superior organizational capacity to detect, document, and escalate information security threats (Siponen & Willison, 2009; Whitman & Mattord, 2018). The finding aligns with the empirical evidence of Orisah-Godfrey and Alikornwo (2026), who demonstrated that information governance strategy was significantly associated with administrative accountability outcomes in Rivers State public sector institutions, suggesting that strategic information governance broadly enhances institutional risk awareness and responsiveness. It also corroborates the findings of Eze and Chukwu (2021), who established that Nigerian public universities with more structured cybersecurity frameworks demonstrated comparatively better risk reporting behaviors than those with fragmented or absent security governance. The moderate to strong correlation coefficient ($r = .641$) suggests that while information security strategy is a substantively important predictor of risk identification efficiency, complementary factors including staff digital literacy, the availability of monitoring technologies, and institutional leadership commitment also contribute to the overall risk identification capacity of tertiary institutions, consistent with the findings of Gbafah (2026) and Alikornwo et al. (2026). The regression coefficient ($B = .503$) further indicates that improvements in information security strategy have a practically meaningful and statistically significant impact on risk identification efficiency, providing strong empirical justification for institutional investments in cybersecurity policy development and data access control systems.

The finding from Hypothesis Two, establishing a significant positive relationship between information security strategy and risk mitigation effectiveness ($r = .618$, $p < .05$; $r2 = .382$), confirms the theoretical predictions of the Enterprise Risk Management Framework, which identifies information and communication infrastructure as foundational enablers of effective risk mitigation capacity in organizations (COSO, 2017; ISO 31000:2018). This finding is consistent with Mbanaso et al. (2022), who established that weak access control protocols and cybersecurity governance

gaps were primary contributors to the persistence of information security risks in Nigerian public institutions, implying that strengthened information security strategy would logically reduce the severity and frequency of these risks. The result further aligns with the empirical evidence of Alikornwo et al. (2026), who found that strategic digital governance investments, including data security protocols and records automation systems, were significantly associated with improved information management outcomes in Rivers State government institutions. The Federal Ministry of Communications and Digital Economy (2024) also reported that the introduction of multi-factor authentication and role-based access control in public institutions was among the most effective technical interventions for reducing data breach incidents, directly corroborating the present study's finding on the relationship between information security strategy and risk mitigation effectiveness. Adeyemi and Oluwaseun (2024) similarly demonstrated that human capital investments in cybersecurity training were significantly associated with improved cybersecurity performance, reinforcing the multi-dimensional nature of effective risk mitigation and the importance of treating information security strategy as a holistic governance construct rather than a purely technical initiative. The regression coefficient (B = .481) indicates that unit improvements in information security strategy yield practically significant gains in risk mitigation effectiveness, providing compelling empirical justification for strategic resource allocation to information security governance in Rivers State tertiary institutions.

CONCLUSION AND RECOMMENDATIONS

This study has provided empirical evidence that information security strategy has a significant positive relationship with administrative risk management in tertiary institutions in Rivers State, Nigeria. Both null hypotheses were rejected at the 0.05 level of significance, with information security strategy accounting for 41.1 percent of the variance in risk identification efficiency and 38.2 percent of the variance in risk mitigation effectiveness. The study's findings are theoretically grounded in the Information Security Management Theory and the Enterprise Risk Management Framework, and are empirically consistent with a substantive body of local and international scholarly evidence on information security governance and administrative risk management in higher education institutions. The study therefore concludes that the deliberate and comprehensive institutionalisation of information security strategy, encompassing cybersecurity policy implementation and data access control mechanisms, is a fundamental governance imperative for tertiary institutions in Rivers State seeking to strengthen their administrative risk management capacity in the face of escalating information security threats. The urgency of this conclusion is underscored by the consistent documentation of institutional information security deficits across Rivers State public institutions in the recent empirical literature (Alikornwo et al., 2026; Orisah-Godfrey & Alikornwo, 2026; Gbafah, 2026; Kalagbor & Adiele, 2026).

Based on the findings and conclusions of this study, the following recommendations are offered with precision:

1. The management of tertiary institutions in Rivers State should develop, formally document, and institutionalise comprehensive information security strategies that explicitly address cybersecurity policy frameworks, data access control standards, incident reporting procedures, staff security responsibilities, and periodic security auditing protocols. These strategies should be reviewed at least biennially to ensure sustained relevance to the evolving information security threat landscape.
2. Tertiary institutions should implement robust data access control systems as a priority governance measure. This includes the adoption of role-based access control frameworks calibrated to job function and authorization level, the deployment of multi-factor

authentication for all institutional information systems, the institutionalisation of regular access rights reviews, and the prompt revocation of access privileges upon the termination of staff or contractor engagements.

3. Institutional managers should invest in regular, structured, and contextually relevant cybersecurity awareness and capacity development programs for all administrative personnel, with particular emphasis on risk identification competencies, phishing awareness, password management hygiene, and incident reporting procedures. Such programs should be designed to bridge the well-documented gap between digital literacy and effective information security practice among administrative staff in Rivers State tertiary institutions.
4. The National Board for Technical Education (NBTE) and the National Universities Commission (NUC) should incorporate information security strategy and administrative risk management as mandatory governance requirements in their institutional accreditation and quality assurance frameworks, thereby creating systemic incentives for all tertiary institutions to invest consistently in information security governance as a core component of administrative management.

REFERENCES

Adeleke, O. J., & Oladipupo, O. A. (2023). Compliance challenges in Nigeria's cybersecurity framework: A systematic review. *International Journal of Information Security and Privacy, 17*(2), 78-95.

Adeyemi, K., & Oluwaseun, A. (2024). The role of human capital in cybersecurity implementation: Evidence from Nigeria. *Cyber Security Review, 12*(3), 112-128.

Adiele, G. C., & Sam-Kalagbor, H. (2026). Bureaucratic decision-making: Leveraging strategic information use in local government councils. BW Academic Journal: *Journal of Contemporary Accounting, Economics and Management, 13*2, 82-94.

Alikornwo, P. M., Sam-Kalagbor, H., & Nyeche, E. (2026). Administrative strategy and public sector effectiveness: The digital information management triangulation. BW Academic Journal: *Journal of Management, Marketing and Accounting Innovations, 10*(1), 78-91.

Alikornwo, P. M. & Nwinyokpugi, P. N. (2025). Administrative communication and decision-making in Public Tertiary Institutions: The mediating role of information management systems. *Journal of Human Resources and Management Science, 10*(7), 89-102.

Alikornwo, P. M., & Adiele, G. C. (2024). Electronic administrative indicators. *Journal of African Innovation and Advanced Studies, 5*(2), 151-160.

Alikornwo, P. M., Adiele, G. C., & Dornanu, L. (2025). Digital transformation: Corollary for administrative decision-making in government ministries. BW Academic Journal 2: *Management, Accounting and Economics Journal, 10*(1), 25-35.

Alikornwo, P. M., Adiele, G. C., & Onyebuenyi, C. I. (2026). Information management in digitally enabled offices: Evaluating administrative productivity in Rivers State government MDAs. BW Academic Journal: *International Journal of Management and Entrepreneurship Research, 11*(2), 29-41.

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

Enofogha, U. (2023). Comparative analysis of cybersecurity strategies, policies, and measures between Nigeria and other nations. *International Journal of Innovative Information Systems and Technology Research, 11*(2), 45-61.

Eze & Nkemdirim (2020). Management of information security in public universities in Nigeria. ResearchGate. https://researchgate.net/publication/341334201

Eze, & Chukwu (2021). Information security risk assessment in public universities. *Nigerian Journal of Information Systems, 9*(1), 44-57.

Federal Ministry of Communications and Digital Economy. (2024). *Nigeria cybersecurity report 2024*. Government Publications, Abuja.

Gbafah, B. L. (2026). Communication and collaboration in relationship to time management in organisation. BW Academic Journal: *In: Corporate Social Responsibility,* 47-52.

Gbafah, B. L. (2026). Digital literacy and secretary's job performance of Rivers State. BW Academic Journal: *In: Corporate Social Responsibility,* 105-112.

Ikuero, A. (2022). A critical review of cybersecurity governance in Nigeria: Policy gaps and implementation challenges. *International Journal of Cybersecurity Policy Research, 4*(1), 22-39.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology: Security techniques - Information security management systems requirements*. ISO.

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

Jacobson, D., & Idziorek, J. (2013). *Computer security literacy: Staying safe in a digital world.* CRC Press.

Justice-Amadi, S. N. (2023). Change management and job performance of office managers in tertiary institutions in Rivers State. *International Journal of Progressive Sciences and Technologies, 39*(2), 155-164.

Justice-Amadi, S. N. (2023). Change management and organizational citizenship behaviour of office managers in tertiary institutions in Rivers State. *International Journal of Progressive Sciences and Technologies, 38*(1), 333-345.

Kalagbor, S. B., & Adiele, G. C. (2026). E-governance and democratic accountability: Assessing the information management capacity of the public sector in Rivers State. BW Academic Journal: *International Journal of Management and Entrepreneurship Research, 11*(2), 96-110.

Mbanaso, U., Chukwudebe, G., Ezeh, G., & Abayomi-Alli, A. (2022). Cybersecurity governance in Nigeria: Challenges and strategic directions. In Proceedings: *Springer Proceedings in Complexity, 21*(2), 355-374.

National Information Technology Development Agency (NITDA). (2020). *Nigeria data protection regulation (NDPR)*. NITDA, Abuja.

Nte, N. D., Enoke, B. K., & Omolara, J. A. (2022). An evaluation of the challenges of mainstreaming cybersecurity laws and privacy protection in Nigeria. *Journal of Law and Legal Reform, 3*(2), 246-266.

Okwu, H. E., Tantua, E., & Obara, C. E. (2023). Enterprise alignment adoption strategies and quality healthcare in South-South Nigeria. *Journal of Office and Information Management (JOIM), 7*(2), 71-91.

Olufowobi, H., Ogunlade, O., & Bello, T. (2019). Cybersecurity practices in Nigerian higher institutions. *Journal of ICT Research, 5*(2), 112-121.

Orisah-Godfrey, L. A. (2026). Leadership communication strategy and administrative staff commitment in educational institutions in Rivers State. BW Academic Journal: *Contemporary Journal of Advancement in Marketing and Management, 13*(2), 42-55.

Orisah-Godfrey, L. A., & Alikornwo, P. M. (2026). Information governance strategy: Assessing the administrative accountability referents in public sector institutions in Rivers State. BW Academic Journal: *International Journal of Accounting, Auditing & Management, 13*(1), 76-88.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information and Management, 46*(5), 267-270.

Ukwandu, E., Okafor, E. N. C., Ikerionwu, C., Olebara, C., & Ugwu, C. (2023). Assessing cybersecurity readiness of Nigeria to Industry 4.0. *Springer Proceedings in Complexity, 21*(2), 355-374.

Whitman, M. E., & Mattord, H. J. (2018). *Management of information security* (6th ed.). Cengage Learning.

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper and Row.