

INFORMATION GOVERNANCE POLICIES AND ORGANIZATIONAL INFONOMICS OF MICROFINANCE BANKS IN SOUTH-SOUTH NIGERIA

ETETE Ephraim Ogumelek and Prof. (Mrs.) A.E. BESTMAN

Department of Office and Information Management, Faculty of Administration and Management, Rivers State University, Port Harcourt, Nigeria

ephraim.etete@ust.edu.ng

Tel: 08068735657

ABSTRACT

This study explored the relationship between information governance policies and organizational infonomics within microfinance banks in South-south Nigeria. Information governance policy is defined as a comprehensive document aligning with corporate governance, involving stakeholders to formalize the management of corporate information assets (Basma, 2019). Organizational infonomics refers to embedding of information values within an organizational culture to achieve operational efficiency and informed decision-making. By focusing on access control and compliance framework policies which are the dimensions of information governance, the study analyzed 211 valid survey responses from 77 banks and found a significant relationship between information governance policies and organizational infonomics. The results further highlight that organizational culture acts as a critical moderator, significantly influencing the strength of the relationship between information governance policies and organizational infonomics. Consequently, the findings emphasize that robust access control and compliance framework policies are essential for driving the success and sustainability of information value that leads to operational efficiency and inform decision making within the Nigerian microfinance banking sector.

Key words: Information governance policy, access control policy, compliance framework policy, inform decision making, operational efficiency organizational infonomics.

INTRODUCTION

In this contemporary time where information serves as the life-wire of an organization (Orok, 2014), effective information governance policies and utilization of information for it to be infonomics to an organization have become very significant for the sustenance and success of any organization that wants to survive in a competitive business environment, which includes the space of microfinance banks operations, as they have been serving as catalysts for financial inclusion and empowerment. This has brought to focus on expounding information governance policies and organizational infonomics of microfinance banks in South-south Nigeria.

Information governance policies are peculiar guidelines, rules, procedures, and standards that formalize the implementation of information governance principles and practices within an organization. It can also be looked at as data protection, freedom of information, information security, retention, disposal, and records management, and subject access request policies which may from time to time be in place within an organization (Law Insider, 2024). According to Crown Records Management (2023) information governance policies are framework that enables organizations to effectively manage their data throughout its lifecycle, and that it covers aspects like data quality, data privacy, data security, and regulatory compliance.

Information governance policies can also be looked at from the perspectives of data governance as most times the concept of data and information are often used interchangeably even if they are not the same as data precedes information. In the perspective of data governance policies, it is a collection of principles, frameworks, programs, roles, and responsibilities that help manage data collection, storage, access, usage, quality, and archival of data assets in its entire life cycle (Atlan, 2024). Information governance policy is a broader concept that encompasses data governance, in a nutshell, data governance policy is inclusive in information governance policies as a combination of data makes up an information that might need policies to put it into effective usage.

Effective information governance policies such as access control and compliance framework policies, ensure regulatory compliance, prevent data breaches, reduce risks, and improve operational efficiency. While information

governance is generic, policies are organization-specific, shaped by an organization's goals and use of its information assets. To achieve an infonomics-oriented organization, these policies must include the key components mentioned. Access control in information governance regulates access to organizational information by mediating requests to resources and determining whether they should be granted or denied (Samarati & Sabrina, 2001). It protects information systems from unauthorized disclosure, alteration, or service denial while ensuring legitimate access (Abdul, Safa, Saja, & Enas, 2020), addressing both insider and outsider threats (Shamil & Jamal, 2018). Effective access control policies include user identification, authentication, authorization, data encryption, and regular audits, and also facilitate information classification.

A compliance framework policy guides organizations in ensuring that information management practices adhere to rules and regulations governing the creation, use, storage, sharing, and destruction of information (Cole, 2024). It provides a structured approach for assessing, implementing, monitoring, and enforcing compliance through mechanisms such as risk assessment, regulatory evaluation, training, policy development, and incident response, embedding regulatory adherence within the organization's data stewardship culture. Embedding information governance policies into organizational culture integrates them into the values, beliefs, and practices that guide how members use and manage information. Such integration shapes employees' behaviors and decision-making, ensuring information is valued, managed effectively, and leveraged strategically to achieve organizational goals, fostering organizational infonomics (Minhaz, 2024).

Infonomics is an approach whereby information is treated as a valuable asset and leveraging it to drive business outcomes, create value, and gain competitive advantage. This is an indication that information should be seen as an organizational asset just like land, machines, employees and the likes. It is about achieving economic resources based on information (Gower, 2012), indicating that it creates wealth for an organization. Infonomics is information obtaining a measurable economic value and other features that qualify it as any other kind of asset, significantly strategic, operational and financial reasons to do so exist (Garifova, 2024). It is the theory, study, and discipline of attributing economic significance to information and data, it strives to apply economic and asset management principles to the valuation, handling, and deployment of information assets (Datagalaxy, 2023). Infonomist proposed information to be intangible organizational assets that are used in the achievement of goals and objective, which manifest in operational efficiency and informed decision making.

Informed decision making emanates from accurate, relevant, and timely information, and organizations use it to achieve its goals and objectives. Informed decisions indicate that decision makers understand the procedures and processes of issues at hand before embarking on relevant actions. It is the process of making choices based on a thorough understanding of available information and it involves gathering, analyzing, and interpreting data to assess potential outcomes and risks (Munir, 2024). Informed decision making is a critical process that has to do with gathering and analyzing data, it is a step-by-step process that enables decision makers to weigh and understand options and choices thoroughly before taking actions, informed decisions enable perfect outcomes in organizations, thereby leading to operational efficiency.

Operational efficiency refers to an organization's ability to optimize processes, resources, and activities to achieve maximum output with minimal input, cost, time, and effort by streamlining workflows, reducing waste, and improving productivity. It involves continuous measurement and improvement of business processes to deliver quality goods and services at the lowest possible cost and in the shortest time (Pipefy, 2023). In relation to organizational infonomics, operational efficiency depends on data-driven decision-making, where information is used to monitor key performance indicators, track process metrics, and identify opportunities for continuous optimization. This underscores the importance of effective information governance policies in enhancing operational efficiency, which forms the basis for examining the relationship between information governance policies and organizational infonomics in microfinance banks in South-South Nigeria.

INFORMATION GOVERNANCE POLICIES

Information governance policies are organization-specific frameworks derived from the broader concept of information governance, designed to guide how information is managed throughout its entire lifecycle, from creation to deletion and destruction. While all organizations require information governance, their policies are unique and tailored to their specific needs, providing principles, standards, procedures, and guidelines for effective information management (Zawiyah, & Azan, 2018). These policies also define data classification, ownership, retention, and accountability, and must incorporate data governance practices, since high-quality information can only be achieved through effective management of data (Munster Technology University, 2021).

Information governance policies are vital to organizations as they address data quality, privacy, security, and regulatory compliance, thereby reducing the risks of data breaches and legal penalties. Effective policies establish clear rules, responsibilities, and standards that safeguard information assets, improve information access and storage, and enhance organizational decision-making through the availability of high-quality information (Casepoint, 2024). By streamlining information use, controlling risks, eliminating data silos, and embedding principles, standards, procedures, and guidelines, information governance policies enable organizations to derive maximum value from their information resources (Halim et al., 2018).

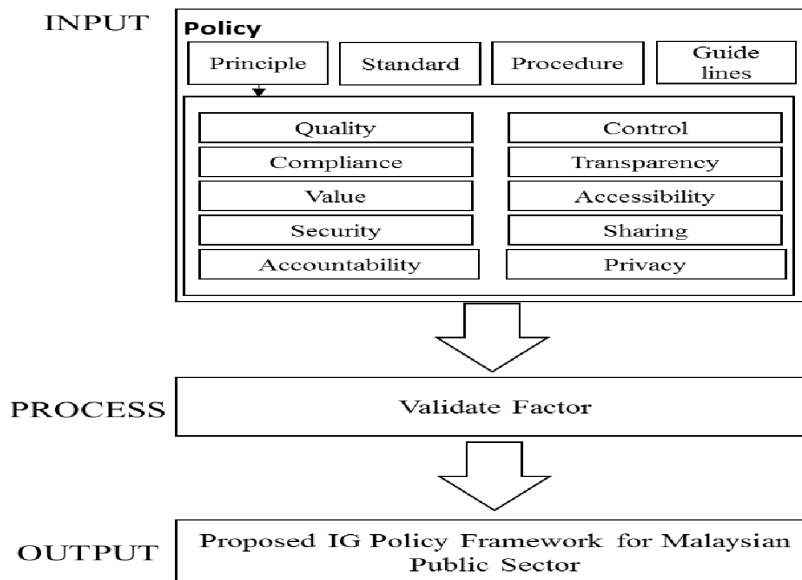


Figure 2.2: Information Governance Policy Framework

Source: Halim et al (2023) Information policies framework for public sector

The information governance framework discussed is based on a study by Malaysian Administrative Modernization and Management Planning Unit (MAMPU). It outlines principles, standards, procedures, and guidelines for public sector information governance policies, emphasizing components like quality, control, value, compliance, transparency, accessibility, security, accountability, sharing, and privacy. This study on microfinance banks in South-south Nigeria adopted components like access control policy and compliance framework policy to test their effect on organizational infonomics.

ACCESS CONTROL POLICY

This is an information governance policy that outlines the rules and procedures for access control within an organization. Access control is a security technique that regulates who or what can view or use resources in a computing environment (Lutkevich, 2023). Access control serves as a proactive defense mechanism, allowing organizations to manage and regulate user access to their digital resources. In the same way that keys and preapproved guest lists protect physical spaces, access control policies protect digital spaces, in other words, they let the right people in and keep the wrong people out (Microsoft, 2023). It is the process of authorizing or restricting access to information, information processing services, and designated physical facilities based on defined permissions. It is the process of mediating every request to resources and data maintained by a system and determining whether the request should be granted or denied (Sabrina & Samarati, 2001). It describes permission available to computing processes (Jaeger, 2007) through a thorough screening of information system users based on the credentials presented to the system for identification.

There are basically two measure approaches in access control (Lutkevich, 2023), and they are physical and logical access control. Physical access control limits access to campuses, buildings, rooms and physical IT assets while logical access control limits connections to computer networks, system files and data. Physical access control is concerned with protecting the physical computer hardware, software, and computing components against destruction by external intruders. This is done by security personnel limiting the activities of persons accessing the building where information system resources are housed. Information system resources are the components

that makes up an information system which according to Zakari, Seidu, & Ekwueme (2020) includes: data, hardware, software, telecommunication network, and people, physical access control can be thought of as physical access to a room with a key. While physical access control is basically concerned with the external environment of information system, logical access control is focused on the use of an information system, which has to do with what is inside the system. Logical access controls are those controls that either prevent or allow access to resources once a user's identity already has been established, and once a user is logged in, they should have access only to those resources required to perform their duties (Taylor, 2013). Access control policy encompasses information system user identification, authentication, authorization, data encryption, information system audit, and securing the physical building that houses the information resources to ensure user responsibility and information system security.

User identification is a fundamental access control process in which a user claims a unique identity to gain access to an organization's information systems and assets (Rouse, 2023). It involves presenting identifiable credentials such as usernames, ID cards, smart cards, passwords, or biometric features, which allow the system to recognize and distinguish users, assign privileges, and track activities (NIST, 2008; Indicative, 2024). User identification addresses key security concerns by confirming who a user is and whether they should be allowed access, using factors based on what a user knows, has, or is, and it serves as a critical step carried out before authentication in securing information systems (Shaffer, 2024).

User authentication is the process of verifying that a user or entity is truly who they claim to be after presenting valid credentials to access an organization's information assets. By requiring users to prove their identity, authentication adds a critical security layer that protects sensitive data and supports the application of the principle of least privilege within organizations (Kyle, 2023; Rajar & Maria, 2019). Common authentication mechanisms include password-based, token-based, and biometric methods, each offering varying levels of security, with passwords relying on secrecy, tokens allowing revocation and expiration, and biometrics using unique biological traits for verification (Nilesh, Salendra, & Mohammed, 2016). To enhance system security, organizations are increasingly implementing multi-factor authentication, which uses multiple verification methods to block unauthorized access even if login credentials are compromised.

User authorization defines the level of access granted to an authenticated user by assigning permissions and privileges based on roles, responsibilities, and the principle of least privilege (Frontegg, 2023). It is a security mechanism that controls access to system resources such as files, applications, data, and services, ensuring that users can only perform actions permitted by their identity and role, and it operates after successful authentication (Hakobyan, 2012). Authorization is essential for the secure operation of information systems and SaaS environments, as it protects sensitive data, limits user activities, and mitigates insider threats by restricting access to what is necessary for job functions. By preventing unauthorized access and supporting data confidentiality, integrity, and reliability often in combination with encryption user authorization forms a critical layer in a defense-in-depth strategy for securing organizational information assets.

Data encryption is a security technique used to protect data during storage and transmission by converting readable data (plaintext) into an unreadable form (ciphertext) that can only be accessed with a secret key or password (De-Groot, 2015). The encryption process involves data, an encryption engine, and key management, where algorithms and keys are used to transform and securely decode information (Sheldon, 2024). Encryption may be symmetric, using a single key for both encryption and decryption, or asymmetric, using a public key for encryption and a private key for decryption (Gibbs, 2024; Smirnoff & Turner, 2019; Brush, 2024). By making unauthorized access extremely difficult, encryption safeguards data at rest and in transit and supports core security objectives such as confidentiality, authentication, integrity, and non-repudiation, thereby protecting information assets and personally identifiable information from misuse or compromise (Sheldon, 2024).

Audit and monitoring are essential access control strategies that ensure only authorized users access information systems and that security violations are detected and addressed promptly. Audit involves the systematic evaluation of access control mechanisms, system activities, and security practices to ensure effectiveness, policy compliance, and alignment with organizational security objectives (Sandhu & Samarati, 1996; Gillis, 2024). This process covers physical security controls, software configurations, information handling practices, and user activities, including the review of logs, audit trails, and incident reports to identify vulnerabilities, policy violations, or insider threats. Monitoring complements audit through the continuous observation and analysis of user sessions and system activities to verify that access controls function as intended (Imprivata, 2021). Monitoring may be

proactive, involving real-time observation when no threat is suspected, or reactive, conducted after a security incident to support investigation and response (Marco, Nicolas, & Giuseppe, 2015).

Compliance Framework Policy

A compliance framework is a structured set of guidelines, processes, systems, and controls that ensures an organization's adherence to relevant laws, regulations, standards, and internal policies governing its operations and activities (McCauley, 2020). It represents a systematic effort to align organizational actions with legal, regulatory, and ethical requirements within the operating environment (Taylor, 2013), while also integrating regulatory demands with organizational goals, identifying risks, and fostering continuous improvement (Anwita, 2024). A well-designed compliance framework is essential for lawful and responsible operations, as it enables organizations to monitor, assess, and mitigate risks, ensure policy adherence, avoid litigation, build credibility and trust, protect stakeholders, enhance efficiency and consistency, and adapt to change, thereby promoting accountability and sustainable organizational performance (Taylor, 2013).

The components of a compliance framework comprise a structured set of guidelines that define how organizations maintain adherence to regulations, standards, and legislation (Abolo, 2023). Despite variations across statutes and frameworks, common elements include governance and leadership commitment, a supportive compliance culture and environment, clearly documented policies and procedures, continuous risk assessment, employee training and competence, effective communication and reporting, monitoring and evaluation mechanisms, and a commitment to continuous improvement (Gentles, 2020). Together, these components provide strategic direction, promote ethical behavior, ensure accountability, identify and mitigate compliance risks, enhance organizational learning, and enable organizations to adapt to changing regulatory and operational environments while sustaining effective and responsible compliance practices.

A compliance framework within information governance policies is essential for organizations of all sizes to ensure legal and regulatory compliance, maintain operational efficiency, and protect their business continuity, particularly in the management of information assets. It provides a systematic approach to managing legal and regulatory risks related to information management, data privacy, security, and confidentiality, while offering a holistic structure for creating and managing enterprise-wide information assets (National Archive of Australia, 2023). A robust information governance compliance framework enhances information quality, usage efficiency, transparency, accountability, and decision-making, thereby supporting organizational infonomics by transforming information into an economic asset. Key components of this framework include alignment with legal and regulatory requirements such as NDPA, FOI Act, GDPR, NHA, and PCI DSS (Manaprasong, 2022), risk assessment and management to mitigate threats like data breaches and unauthorized access, policy development and documentation to standardize information practices (Pratt, 2024), monitoring and enforcement to ensure adherence and accountability (Lakum, 2023), training and awareness to promote employee compliance and reduce legal liability (Movchan, 2024), and incident response remediation to address security breaches and ensure business continuity through structured response processes (Intersec, 2024).

ORGANIZATIONAL INFONOMICS

Organizational infonomics is the strategic management of information as a valuable organizational asset, applying economic principles to maximize its value. It involves valuing information, assessing its impact, and making informed decisions to optimize its use, thereby treating information as a critical resource alongside traditional assets like capital and labor. It entails making an organization's information to be infonomics in nature. Which According to Regazzi (2013) is underlying the value of information in terms of its production, market demand, and economic impact.

Infonomics, first coined by Douglas Laney in the 1990s, emphasizes treating information as a valuable economic asset similar to capital or labor. Laney proposed that organizations should apply the three pillars of infonomics which are monetize, manage, and measure to extract economic value from information, improve operational efficiency, and enhance business outcomes such as production, sales, and innovation (Laney, 2018). Other scholars have expanded the concept, defining infonomics as an enterprise management discipline that values and accounts for information as an asset, on par with financial, physical, or human capital (Regazzi, 2013; Rouse, 2015; Satori, 2022). Across definitions, the focus remains on leveraging information to generate tangible and intangible benefits for organizations.

The three pillars of infonomics guide how information is handled within organizations. Monetization involves recognizing the economic potential of information, whether through direct sale, cost reduction, productivity gains,

or competitive advantage. Managing information focuses on strategic oversight across the information lifecycle, ensuring quality, integrity, security, and alignment with organizational goals. Measuring information quantifies its impact using financial, operational, and strategic metrics, helping organizations understand the value of information in decision-making, process efficiency, and performance outcomes (Laney, 2018).

Valuation models in infonomics include foundational and financial approaches. The foundational approach assesses intrinsic value, business value, and performance value, focusing on the usefulness, strategic contribution, and operational effectiveness of information. The financial approach evaluates cost, market, and economic value, examining expenses, market demand, and overall impact on organizational revenue and objectives. By applying these principles, organizational infonomics enables informed decision-making, innovation, and operational efficiency, ultimately maximizing the economic returns and strategic benefits of information assets. This study examines how these concepts manifest in microfinance banks in South-South Nigeria.

Informed decision making

It involves making choices based on accurate, relevant, and timely information. It combines knowledge and cognitive evaluation to select the best course of action among alternatives, reducing the risk of poor outcomes (Olivier, 2012; Sharma, 2023; Birt, 2022). Effective informed decisions result in positive organizational outcomes, such as increased productivity, profitability, and customer satisfaction, and reflect the economic value of information assets, a concept aligned with organizational infonomics (Gabriel & Obara, 2013). Key components that support informed decision making include: information availability and accessibility, information quality, and analysis and interpretation of information. Availability and accessibility ensure that relevant data is obtainable when needed, often supported by management information systems (MIS), which collect, process, store, and transmit information to facilitate decision-making (Khazanchi, 2009; Adepoju, 2014; Laudon & Laudon, 2007; Gabriel & Obara, 2013). Information quality emphasizes accuracy, reliability, completeness, relevance, and timeliness, which are essential for sound decisions (Alshikhi & Abdullah, 2018; Wang & Strong, 1996; Global Justice Information Sharing Initiative, 2007). Analysis and interpretation transform raw data into actionable insights through processes such as collection, storage, documentation, analysis, and reporting (AQR Glossary, 2022; Maksud, 2023; Simplilearn, 2023).

Strategic planning and innovation are additional pillars of informed decision making. Strategic planning defines organizational goals and priorities and guides resource allocation and decision-making (Terrell, 2024). Innovation, triggered by strategic planning, introduces new ideas, processes, products, or services that create value and drive organizational growth, whether through sustaining or disruptive innovations (Boyles, 2022). Informed decision making within organizational infonomics integrates these elements, enabling leaders to leverage information assets, optimize operations, manage risks, and enhance overall efficiency and effectiveness.

Operational efficiency

It is the ability of an organization to maximize output while minimizing input, resources, or effort, enabling timely and cost-effective delivery of goods and services (Cook, 2024). Within the framework of organizational infonomics, leveraging information as a strategic asset allows organizations to make informed decisions that drive operational efficiency, enhance innovation, and create competitive advantage. By effectively using information assets, organizations can reduce waste, optimize processes, allocate resources efficiently, and improve overall performance. The key factors contributing to operational efficiency include waste minimization, process optimization, and effective resource allocation. Minimizing waste involves reducing time, materials, energy, and effort through streamlined operations, while process optimization standardizes procedures, automates repetitive tasks, and improves workflows to enhance quality and reduce costs (Numminen, 2023). Effective resource allocation ensures that human, financial, material, technological, and informational resources are deployed optimally, maximizing output and preventing inefficiencies or staff burnout (Stearns, 2023; Shwartz, 2023; Subramanian, 2019).

Technology and supply chain optimization further enhance operational efficiency as information and communication technologies enable managers to analyze data, streamline communication, monitor supply chains, and make timely operational decisions. Supply chain optimization involves refining the entire network of activities, including inventory, suppliers, logistics, and demand forecasting, to minimize costs, reduce lead times, and improve customer satisfaction (Zhou, 2023). Access to high-quality information is critical across these areas, allowing organizations to coordinate operations, allocate resources effectively, and achieve strategic goals efficiently.

METHODS

This study adopted a survey design to collect data and a correlational approach to examine the relationship between information governance policies and organizational infonomics in microfinance banks in South-South Nigeria. The research focused on 95 microfinance banks licensed by the Central Bank of Nigeria across Rivers, Delta, Akwa Ibom, Edo, Bayelsa, and Cross River state. The study used simple random sampling to select 77 microfinance banks from a population of 95 in South-South Nigeria, determined using Taro Yamane's formula with a 5% margin of error. Three personnel from each bank totaling 231 participants, including CEOs, directors, officers, and IT staff were randomly chosen to ensure representative coverage of the sector and its information assets. This diverse sample provided a reliable basis for analyzing the study's objectives.

In this study, the reliability of the research instrument was assessed through internal consistency using Cronbach's alpha coefficient, as it is widely recognized for determining the fitness of research scales and questionnaires (Taber, 2017). Cronbach's alpha represents the average reliability that would be obtained from all possible split-half measurements, making it a robust method for evaluating the consistency of the structured questionnaire used in the study (Finchilescu, 2002). Below is the table showing the reliability of variables in the study:

Table 3.1: Cronbach's Alpha Reliability

S/No.	Variables	Number of items	Number of cases	Cronbach's Alpha
1.	Access Control Policy	4	211	0.823
3.	Compliance Framework Policy	4	211	0.789
5.	Organizational Culture	4	211	0.805
6.	Informed Decision	4	211	0.801
7.	Operational Efficiency	4	211	0.775

Source: SPSS 22 Cronbach's Alpha

The table shows the reliability results of the study variables using Cronbach's Alpha. Each variable was measured with four items and tested on 211 respondents. The Cronbach's Alpha values range from 0.775 to 0.823, all exceeding the acceptable threshold of 0.70, indicating good internal consistency. This means the questionnaire items for all variables are reliable and suitable for further analysis.

The study used both descriptive and inferential statistical analyses, conducted with IBM SPSS version 20. Descriptive analysis summarized and organized the data using mean scores to indicate levels (low to very high) and standard deviation to show variability. Inferential analysis included bivariate analysis with Spearman Rank Order Correlation to assess the strength and direction of relationships between variables, and multivariate analysis with partial correlation to examine the moderating effect of organizational culture on the relationship between information governance policies and organizational infonomics. This approach provided a comprehensive evaluation of relationships and interactions among study variables.

Descriptive Analysis

The study employed univariate descriptive analysis to examine information governance policies and organizational infonomics of microfinance banks in South-South Nigeria, using mean and standard deviation to describe the central tendency and variability of each variable. Data were collected through a structured questionnaire based on a 5-point Likert scale, with a criterion mean of 3.00 used to interpret responses as low, average, or high (Ahiauzu and Asawo, 2016). The analysis focused on access control and compliance framework as predictors of information governance policies, while informed decision-making and operational efficiency measured organizational infonomics, with organizational culture serving as a moderating variable. Below are tables showing the descriptive analysis:

Table 1: Respondents Rates for Access Control Policy

	N	Min.	Max.	Sum	Mean	Std. Dev.
User identification and authentication prevents authorize access to your organization's information assets.	211	1.0	5.0	897.0	4.25	.861
User authorization supports role-based access control and thereby leads to information asset protection.	211	1.0	5.0	884.0	4.19	.982
Data encryption enables safe information storage and sharing thereby prevents unauthorize access to information access in your organization.	211	1.0	5.0	870.0	4.12	.973
Regular conducts of audit and monitoring enables compliance with access control policies.	211	1.0	5.0	898.0	4.26	.787
Valid N (listwise)	211					

Source: *Research Survey, 2024*

The table presents respondents' ratings on access control policy items based on 211 valid responses. The mean scores for all items range from **4.12 to 4.26**, which are well above the criterion mean of 3.00, indicating a high level of agreement among respondents. This suggests that user identification and authentication, user authorization, data encryption, and regular audit and monitoring are perceived as effective in protecting organizational information assets and ensuring compliance with access control policies. The standard deviation values, ranging from **0.787 to 0.982**, show relatively low variability in responses, indicating consistency in respondents' views. Overall, the table reflects a strong and positive perception of access control policies in the studied organizations.

Table 3: Response Rate for Compliance Framework Policy

	N	Min.	Max.	Sum	Mean	Std. Dev.
Information governance policies aligns with legal regulations and industry standards in your organization.	211	1.0	5.0	896.0	4.25	.848
Information governance policy compliance framework in your organization ensures risk assessment and management.	211	1.0	5.0	882.0	4.18	.988
A well-developed and documented information governance policy enables information asset valuation.	211	1.0	5.0	863.0	4.09	1.003
Effective monitoring and enforcement of information governance policies ensures compliance to usage of your organizations information asset.	211	1.0	5.0	886.0	4.20	.866
Valid N (listwise)	211					

Source: *Research Survey, 2024*

The descriptive analysis of four compliance framework items shows strong agreement among respondents, with all mean scores above 4 on a 5-point Likert scale. The highest mean (4.25) was for alignment of information governance policies with legal and industry standards, while the lowest (4.09) was for enabling information asset valuation. Standard deviations indicate relatively consistent responses, particularly for policy alignment (0.866), though asset valuation showed slightly more variation (1.003). Overall, respondents perceive compliance frameworks as effective in ensuring legal alignment, risk management, asset valuation, and enforcement of information governance policies within microfinance banks.

Table 3: Response Rate on Organizational Culture

	N	Min.	Max.	Sum	Mean	Std. Dev.
The culture of your organization values information as a strategic asset and integrates it into decision-making processes.	211	1.0	5.0	897.0	4.25	.867
Leaders demonstrate and promote a culture of transparency, accountability, and ethical behavior in projecting information governance policies in your organization.	211	1.0	5.0	886	4.20	.960
In your organization, information is shared freely and openly across departments and levels, to support collaboration and informed decision-making.	211	1.0	5.0	862.0	4.09	1.025
Prioritization of privacy and adherence to ethical standards in handling and processing data enables information assets valuation.	211	1.0	5.0	891.0	4.22	.841
Valid N (listwise)	211					

Source: *Research Survey, 2024*

The descriptive analysis of four organizational culture items shows strong agreement among respondents, with all mean scores above 4 on a 5-point Likert scale. The highest mean (4.25) was for valuing information as a strategic asset, while the lowest (4.09) was for sharing information openly across departments. Standard deviations indicate consistent responses, particularly for prioritizing privacy and ethical standards (0.841), though information sharing showed more variation (1.025). Overall, respondents perceive their organizational culture as valuing information, promoting transparency, ethical behavior, and integration of information into decision-making, highlighting its key role in supporting effective information governance.

Table 4: Response Rate on Informed Decision Making

	N	Min.	Max.	Sum	Mean	Std. Dev.
In your organization, information is readily available and accessible to support decision making.	211	1.0	5.0	894.0	4.24	.889
Your organization's information is accurate, reliable, and up-to-date, enabling informed choices towards achieving goals and objectives.	211	1.0	5.0	884	4.19	.982
The analysis and interpretation of information within your organization are effective for making informed decisions.	211	1.0	5.0	870.0	4.12	.973
Strategic planning and innovation in your organization are significantly influenced by the availability of accurate and timely information.	211	1.0	5.0	895.0	4.24	.818
Source: <i>Research Survey, 2024</i>	211					

The descriptive analysis of four informed decision-making items shows strong agreement among respondents, with all mean scores above 4 on a 5-point Likert scale. The highest means (4.24) were for information availability and accessibility and its influence on strategic planning and innovation, while the lowest (4.12) was for effective analysis and interpretation of information. Standard deviations indicate relatively consistent responses, particularly for strategic planning and innovation (0.818), though information accuracy showed slightly more variability (0.982). Overall, the results suggest that employees perceive organizational information as accessible, accurate, and reliable, supporting effective decision-making and fostering organizational infonomics.

Table 5: Response Rate for Operational Efficiency

	N	Min.	Max.	Sum	Mean	Std. Dev.
Your organization has implemented effective processes to minimize waste, reduce unnecessary costs, and optimize resource utilization	211	1.0	5.0	881.0	4.18	.961
Your organization continuously reviews and optimizes its processes to improve productivity, reduce inefficiencies, and enhance overall performance	211	1.0	5.0	864	4.09	1.100
Resources (such as personnel, equipment, and budget) are allocated effectively and efficiently to support organizational goals and objectives.	211	1.0	5.0	859.0	4.07	1.014
My organization leverages on technology to effectively streamline processes, improve productivity, and enhance overall operational efficiency	211	1.0	5.0	895.0	4.24	.789
Valid N (listwise)	211					

Source: *Research Survey, 2024*

The table indicates that respondents generally perceive a high level of operational efficiency in their organizations, with all items recording mean scores above 4.00 on a 5-point Likert scale. Leveraging technology to streamline processes and enhance productivity received the highest agreement and the most consistent responses, while effective resource allocation, though slightly lower, was still positively rated. Overall, the results show strong consensus that organizations effectively optimize processes, utilize resources efficiently, and apply technology to improve productivity, highlighting the important role of operational efficiency in supporting organizational infonomics and achieving strategic objectives in the microfinance banking sector.

Inferential Analysis

The inferential analysis carried out in the study is bivariate and multivariate analysis, bivariate analysis examines the relationship between two variables to determine how the outcome variable is influenced by the explanatory variable (Alessandro, Paola, Russo, & Fabio, 2018). In this study, it was used to explore the associations between dimensions of information governance policies and organizational infonomics in South-South Nigerian microfinance banks. While multivariate analysis refers to a set of statistical techniques used to analyze data that involves multiple variables. It is concerned with the analysis of simultaneous relationship among there or more variables or phenomena (Shukla, 2018). Below are tables showing bivariate and multivariate analysis in the study:

Table 5: *Correlations between Access Control and Informed Decision Making*

		Access Control	Inform Decision Making
Spearman's rho	Access Control Policy		
	Correlation	1.000	.983**
	Coefficient		
	Sig. (2-tailed)	.	.000
	N	211	211
	Inform Decision Making		
	Correlation	.983**	1.000
	Coefficient		
	Sig. (2-tailed)	.000	.
	N	211	211

** . Correlation is significant at the 0.01 level (2-tailed).

Source: *Research Survey, 2024*

The table above shows the Spearman's rank-order correlation between Access Control and Informed Decision Making. The correlation coefficient of 0.983 indicates a very strong positive relationship, meaning that better access control is closely associated with more effective informed decision-making. The relationship is statistically significant ($\rho = 0.01 < 0.05$), leading to the rejection of the null hypothesis (H_0) and the acceptance of the alternative hypothesis that a strong relationship exists between these variables in South-South Nigerian microfinance banks.

Table 6: *Correlations between Access Control and Operational Efficiency*

		Access Control	Operational Efficiency
Spearman's rho	Access Control Policy		
	Correlation	1.000	.895**
	Coefficient		
	Sig. (2-tailed)	.	.000
	N	211	211
	Operational Efficiency		
	Correlation	.895**	1.000
	Coefficient		
	Sig. (2-tailed)	.000	.
	N	211	211

** . Correlation is significant at the 0.01 level (2-tailed).

Source: *Research Survey, 2024*

The table above shows the Spearman's rank-order correlation between Access Control and Operational Efficiency. The correlation coefficient is 0.895, indicating a very strong positive relationship: as access control improves, operational efficiency also increases. The relationship is statistically significant at the 0.01 level (2-tailed), with a significance value of 0.000, and is based on data from 211 respondents. This suggests that effective access control policies are strongly associated with higher operational efficiency in the surveyed microfinance banks.

Table 5: *Correlations between Compliance Framework and Informed Decision Making*

		Compliance Framework	Informed Decision
Spearman's rho	Compliance Framework Policy	Correlation Coefficient	1.000
		Sig. (2-tailed)	.000
		N	211
	Informed Decision	Correlation Coefficient	.962**
		Sig. (2-tailed)	.000
		N	211

** . Correlation is significant at the 0.01 level (2-tailed).

Source: *Research Survey, 2024*

The table above shows the Spearman’s rank-order correlation between Compliance Framework and Informed Decision Making. The correlation coefficient is **0.962**, indicating a very strong positive relationship: better compliance framework practices are closely associated with more effective informed decision-making. The relationship is statistically significant at the 0.01 level (2-tailed), with a significance value of **0.000**, based on 211 respondents. This suggests that robust compliance frameworks strongly support informed decision-making in the surveyed microfinance banks.

Table 7: *Correlations between Compliance Framework and Operational Efficiency*

		Compliance Framework	Operational Efficiency
Spearman's rho	Compliance Framework Policy	Correlation Coefficient	1.000
		Sig. (2-tailed)	.000
		N	211
	Operational Efficiency	Correlation Coefficient	.879**
		Sig. (2-tailed)	.000
		N	211

** . Correlation is significant at the 0.01 level (2-tailed).

Source: *Research Survey, 2024*

The table above shows a strong, positive correlation between Compliance Framework Policy and Operational Efficiency. Using Spearman’s rho, the correlation coefficient is **0.879**, which is statistically significant at the **0.01 level (p = 0.000)**. This indicates that higher adherence to compliance frameworks is strongly associated with improved operational efficiency among the 211 respondents surveyed.

How Organizational Culture moderates the relationship between Information Governance Policies and Organizational Infonomics

Control Variables			Information Governance Policy	Organizational Infonomics	Organizational Culture
		Correlation	1.000	.977	.981
	Information Governance Policy	Significance (2-tailed)	.	.000	.000
		df	0	209	209
		Correlation	.977	1.000	.967
-none ^a	Organizational Infonomics	Significance (2-tailed)	.000	.	.000
		df	209	0	209
		Correlation	.981	.967	1.000
	Organizational Culture	Significance (2-tailed)	.000	.000	.
		df	209	209	0
		Correlation	1.000	.570	
	Information Governance Policy	Significance (2-tailed)	.	.000	
Organizational Culture		df	0	208	
		Correlation	.570	1.000	
	Organizational Infonomics	Significance (2-tailed)	.000	.	
		df	208	0	

a. Cells contain zero-order (Pearson) correlations.

Source: *Research Survey, 2024*

The table above illustrates that Organizational Culture is a significant moderator in the relationship between Information Governance Policies and Organizational Infonomics. The initial zero-order Pearson correlation indicates a near-perfect positive relationship of **.977** between the two primary variables when no controls are applied. However, when Organizational Culture is introduced as a control variable, this correlation drops significantly to **.570**, although it remains statistically significant ($p = .000$). This substantial decrease in the correlation coefficient confirms that while Information Governance Policies have a direct impact on Organizational Infonomics, the strength and effectiveness of that relationship are heavily dependent on the moderating influence of the organization's culture.

DISCUSSION OF FINDINGS

This study demonstrated a strong and statistically significant positive relationship between information governance policies and the organizational infonomics of microfinance banks in South-South Nigeria. Information governance policy is defined as a comprehensive document that involves stakeholders to formalize the management of corporate information assets in alignment with corporate governance (Basma, 2019). Inferential analysis using Spearman's rank-order correlation reveals that access control policy is exceptionally closely associated with informed decision-making, yielding a very strong correlation coefficient of 0.983. Additionally, access control correlates highly with operational efficiency at 0.895, leading to the rejection of the null hypothesis and the conclusion that effective governance dimensions are primary drivers for information-based value in the microfinance banking sector.

Furthermore, the results highlight that organizational culture significantly moderates the strength of the relationship between information governance policies and organizational infonomics. While generic information governance takes the same shape across various settings, effective governance policies must be specific to an organization's nature, goals, and objectives. For a microfinance bank to become "infonomics in nature," it must integrate specific components such as information classification, data stewardship, and compliance framework policies. Embedding these policies within the organizational culture not only ensures regulatory compliance and prevents data breaches but also minimizes risks and enhances overall operational efficiency through better-informed decision-making.

CONCLUSION

The study shows that strong information governance policies such as access control and compliance frameworks policy significantly improve organizational infonomics in microfinance banks in South-South Nigeria. These policies enhance decision-making, operational efficiency, and information security, accuracy, and accessibility. Additionally, a supportive organizational culture amplifies these benefits, making comprehensive information governance essential for the banks' sustainability and success.

RECOMMENDATION

1. Microfinance banks should strengthen access control by using robust authentication, user identification, and regular access audits to protect sensitive customer and financial information.
2. Microfinance banks should align information governance with legal and industry standards to ensure accurate, compliant decision-making and reduce regulatory risks.
3. Fostering a culture that values information governance through employee training and awareness is essential for organizational success.

REFERENCE

- Abdul S., A. (2020). *Access control security review: concept and models*. https://www.researchgate.net/publication/346021492_Access_Control_Security_Review_Concepts_and_Models?
- Abolo, E. (2023). *Developing a compliance framework. The risk management academy limited*. www.theriskacademy.org
- Ahiauza, A. I. & Asawo, S. P. (2016). *Advanced social research methods*. Port Harcourt: CIMRAT Publications
- AQR Glossary (2022). *Analysis and interpretation*. <https://www.aqr.org.uk/glossary/analysis-and-interpretation>
- Anwita D. (2024). *A quick overview of compliance framework*. <https://sprinto.com/blog/compliance-framework/>
- Alshikhi, O. A. & Abdulla, B. M. (2018). Information quality; definition, dimension, measurements, and relationship with decision making. *European Journal of Business and Innovation Research*. Vol.6, No.5, pp.36-42, October 2018. <https://www.eajournals.org/wp-content/uploads/Information-Quality-Definitions-Measurement-Dimensions-and-Relationship-with-Decision-Making-6.pdf>

- Atlan (2024). *Data governance policies: example, template, and how to write one*. <https://atlan.com/data-governance-policies/>
- Basma, M. (2019). An information governance policy is required for my institution, what to do? Practical method and tool enabling efficient management for corporate information assets. DOI: 10.4018/978-1-5225-7080-6.ch003
- Boyles, M. (2022). *Innovation in Business: What It Is & Why It's So Important*. *Business Insights Blog*. <https://online.hbs.edu/blog/post/importance-of-innovation-in-business>
- Birt, J. (2022). *How to make informed decision, 6 steps tips and examples*. <https://www.indeed.com/career-advice/career-development/informed-decision>
- Brush, K. (2024). Asymmetric cryptography. <https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography>
- Casepoint (2024). *Goals of information governance: why it is important*. <https://www.casepoint.com/resources/spotlight/goals-of-information-governance-why-is-it-important/>
- Cole, B. (2024). *Compliance framework*. <https://www.techtarget.com/searchcio/definition/compliance-framework>
Compliance framework: a detailed guide. <https://www.theknowledgeacademy.com/blog/compliance-framework/>
- Cook, B. (2024). *What is operational efficiency and how can you improve it?* <https://tipalti.com/financial-operations-hub/operational-efficiency/>
- Coutinho, A. (2023). *The importance of a strong compliance culture*. <https://www.linkedin.com/pulse/importance-strong-compliance-culture-adriano-coutinho-mba-cams/>
- Crown Records Management (2023). *How to guide and create an information governance policies*. <https://www.crownrms.com/insights/a-how-to-guide-on-creating-an-information-governance-policies/>
- Datagalaxy (2023). *Infonomics: monetize, manage, and utilize data set as an asset*. <https://www.datagalaxy.com/en/blog/infonomics-data-as-an-asset/>
- De-Groot, J. (2015). What is data encryption? (definition, best practices and more) <https://www.fortra.com/blog/what-data-encryption>
- Finchilescu, G. (2002). Measurements. In C. Tredoux & K. Durrheim (Eds.), *Numbers, hypotheses & conclusions: A course in statistics for the social science* (pp. 201-229). Cape Town: University of Cape Town Press.
- Frontegg (2023). *All you need to about user authorization*. <https://frontegg.com/blog/user-authorization>
- Gabriel, J., & Obara, C. (2013). Management information system and corporate decision making – Making: Literature review. *The International Journal Of Management, Vol 2 Issue 3 (July, 2013)* www.theijm.com
- Garifova, F. (2024). *Infonomics and The Value of Information in The Digital Economy*. 2nd Global Conference on Business, Economics, Management and Tourism, 30-31 October 2014, Prague, Czech Republic <https://core.ac.uk/download/pdf/82100027.pdf>.
- Gentle, A. (2020). Eight essential components of compliance risk management. <https://www.firstreference.com/blog/8-essential-components-of-compliance-risk-management/>

- Gibbs M. (2024). *Symmetric encryption: definition and example*. <https://study.com/academy/lesson/symmetric-encryption-definition-example.html>
- Global Justice information Sharing Initiative (2007). *Information quality: the foundation for justice decision making*. www.it.ojp.gov/iq_resources
- Gower, R. (2012). *What is infonomics*. <http://www.infonomics.ltd.uk/blog/2012/12/06/what-is-infonomics/>
- Hakobyan, D. (2012). Authentication and authorization system in cloud environment. <https://www.diva-portal.org/smash/get/diva2:557150/fulltext01.pdf>
- Halim, N, Zawiyah Y, & Azan M. (2018). The requirement for information governance policies framework in Malaysian public sector. *International Journal of Engineering & Technology*, 7 (4.15) (2018) 235-239 DOI: 10.14419/ijet.v7i4.15.22996 <https://blog.firstreference.com/8-essential-components-of-compliance-risk-management/>
- Intersec (2024). *Incident response remediation*. <https://www.intersecworldwide.com/incident-response-remediation>
- Jaeger, P.T. (2007). Information policy, information access, and democratic participation: Thenational and international implications of the Bush administration's information policies. *Government Information Quarterly*, 24, 840-859.
- Imprivata (2021), *What is Access Monitoring*. <https://www.imprivata.com/uk/node/103686>
- Khazanchi, D. (2009). Handbook of Research on Information Security and Assurance. DOI: 10.4018/978-1-59904-855-0.ch019
- Kyle, J. (2023). Six user authentication types to secure network. https://media.bitpipe.com/io_10x/io_102267/item_1306461/E-guide_6_user_authentication_types_to_secure_networks.pdf
- Lakum, C. (2023). What is compliance and monitoring, and best practices for implementation. <https://www.linkedin.com/pulse/what-c-ompliance-monitoring-best-practices-chirag-lakum/>
- Laney, D. (2018). *Infonomics: How to monetize, manage, measure information as an asset for competitive advantage*. Bibliomotion, Inc, 711 Third Avenue New York, NY 10017, USA
- Laudon, K.C. and Laudon, J.P. (2007) *Management Information Systems: Managing the Digital Firm*. 9th Edition, Pearson/Prentice Hall, Upper Saddle River, 145-278.
- Law Insider (2024). *Information governance definitions*. <https://www.lawinsider.com/dictionary/information-governance-policies>
- Law Insider (2024). Information handling system definition. <https://www.lawinsider.com/dictionary/information-handling-system>
- Lutkevich, B. (2023) What is Access Control List (ACL)? <https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL>
- MacCauley M. (2020). *Three steps to building a compliance framework*. <https://www.linkedin.com/pulse/3-steps-creating-compliance-framework-marissa-mccauley/>
- Mikalef, P., Maria B., Lekakos, G., & Krogstie, J. (2020). The role of information governance in big data analytics driven innovation. *International Journals of Information Systems Applications*. <https://doi.org/10.1016/j.im.2020.103361>

- Manaprasong S. (2022). *Align with the law; expert legal advice and compliance solution*. <https://personnel.obec.go.th/home/archives/412625>
- Marco, A., Nicolas, P., & Giuseppe, S. (2015). *Percival: proactive and reactive attack and response assessment for cyber incidents using visual analytics*. 2015 IEEE Symposium on Visualization for Cyber Security (VIZSEC). DOI:[10.1109/VIZSEC.2015.7312764](https://doi.org/10.1109/VIZSEC.2015.7312764)
- Microsoft (2023). What is access control? <https://www.microsoft.com/en-us/security/business/security-101/what-is-access-control>
- Minhaz M. (2024). *Organizational culture: definition, characteristics, roles, types*. <https://www.iedunote.com/organizational-culture>
- Movchan S. (2024). What is compliance training? <https://raccoongang.com/blog/what-compliance-training/>
- Munir A. (2024). *Big data analytics techniques for market intelligence*. DOI: 10.4018/979-8-3693-0413-6.ch013
- Nilesh, A., Salendra P., & Mohammed, F. (2016). A review of authentication methods. *International Journal of Scientific & Technology Research*, Volume 5, ISSUE 11, November 2016 ISSN 2277-8616
- Nummenie L. (2023). *Process optimization explained, methods, benefits and tools*. <https://www.workfellow.ai/learn/what-is-process-optimization>
- Olivier, S. (2012). *Knowledge solutions. On decision making*. <https://www.adb.org/sites/default/files/publication/30024/decision-making.pdf>
- Orok, B. (2014). Security consideration in information management of organization. *Global Management of Business Research: Administration and Management*. Volume 14. Online ISSN: 2249-4588 & Print ISSN: 0975-5853 <https://journalofbusiness.org/index.php/GJMBR/article/download/1259/1169>
- Pipefy (2023) *Operational Efficiency: Definition, Examples, and Strategies*. Pipefy Blog. <https://www.pipefy.com/blog/operational-efficiency/>
- Pratt, M. (2024). *Data governance policies*. <https://www.techtarget.com/searchcio/definition/data-governance-policies>
- Regazzi, J. (2013). *Infonomics and Value Creation in the New Business of Free*. John J. Igi Global, p.305.
- Rouse, M. (2015). *What does infonomics means?* <https://www.techopedia.com/definition/30877/infonomics>
- Rouse, M. (2018). *Information sharing*. <https://www.techopedia.com/definition/24839/information-sharing>
- Samarati, P. & Sabrina C. (2001). *control: policies, models and mechanisms*. https://link.springer.com/content/pdf/10.1007/3-540-45608-2_3.pdf
- Satori (2022). *Infonomics*. <https://satoricyber.com/glossary/infonomics/>
- Shaffer (2024). What Is User Authentication? A Guide for Modern Apps. <https://frontegg.com/blog/authentication>
- Sheldon, R. (2024). *Data lifecycle management (DLM)*. <https://www.techtarget.com/searchstorage/definition/data-life-cycle-management>
- Shukla, T. (2018). *Introduction to multivariate data analysis*. https://www.researchgate.net/publication/328857958_Introduction_to_Multivariate_Data_Analysis

- Shwartz, B. (2023). *Organizational resources basics: managing company resources*. <https://www.projectmanager.com/blog/organizational-resources>
- Smirnoff, P. and Turner, D.M. (2019). *Cryptomathic symmetric key encryption-why, where, and how it is used in banking*. <https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking>
- Stearns, J. (2023). *Resource allocation in economics, definitions, benefits, and process*. <https://study.com/academy/lesson/resource-allocation-in-management-methods-process-strategy.html>
- Subramanian, V. (2019). *Five major resources needed by a company- what do you think is the most important?* <https://www.linkedin.com/pulse/5-major-resources-needed-company-what-do-you-think-most-subramanian/>
- Taber, K. (2017). *The use of Cronbach's alpha when developing and reporting research instruments in science education*. *Res Sci Educ* (2018) 48:1273–1296 DOI 10.1007/s11165-016-9602-2
- Taylor, P. L. (2013) *Preparing the System Security. FISMA Compliance Handbook* , 2013 pp 167-199
- Terrell H. (2024). *Strategic Planning*. <https://www.techtarget.com/searchcio/definition/strategic-planning>
- Wang, R. and Strong, D. (1996). Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems*, 12(4), pp.5-33
- Wegel M., Kamenowski M., & Andrea B. (2018). *Compliance and value orientation at universities*. <https://ul.qucosa.de/api/qucosa%3A32049/attachment/ATT-0/>
- Wendelborn, C., Anger M., & Schikhardt, C. (2023). What is data stewardship: towards a comprehensive understanding. *Journal of Biomedical Informatics* 140(5p2):104337 DOI:[10.1016/j.jbi.2023.104337](https://doi.org/10.1016/j.jbi.2023.104337)
- Zakari, M., Seidu O., & Ekwueme L. (2020). *Course Guard: information system, resources, and services*. National Open University of Nigeria Headquarters University Village Plot 91, Cadastral Zone Nnamdi Azikiwe Expressway Jabi, Abuja. © 2020 by NOUN Press https://nou.edu.ng/coursewarecontent/LIS%20105_0.pdf
- Zhou, A. (2023). *Supply chain optimization, what is it & best practices*. <https://archive.gofreight.com/blog/solution/supply-chain-optimization-what-is-it-best-practices.html>