Academic Scholars Publishing League (ASPL)
International Journal of Management Sciences
ISSN: 2360-9944 | Volume 11, Issue 10 | November, 2023| pages 175 – 193
DOI: 2775-145-62-111013
arcnjournals@gmail.com
https://arcnjournals.org

Information Accountability and Access Control of Deposit Money Banks in Port Harcourt, Rivers State

Akere, Catherine Barikuma
Department of Office and Information Management, Rivers State University

Abstract: *This study examined the relationship between information accountability and access control of deposit money banks in Port Harcourt. The study adopted the cross-sectional research survey design. Primary data was generated through structured questionnaire. The population of the study consisted of 80 respondents who were randomly selected from 20 deposit money banks in Port Harcourt. The entire population of 80 was retained as the sample since it was relatively small and manageable. The hypotheses were tested using the Spearman's Rank Order Correlation Statistics. The tests were carried out at a 0.05 significance level. The findings revealed that there is a positive and significant relationship between information accountability and access control. Therefore, the study concludes that information accountability positively enhances access control of deposit money banks in Port Harcourt. Hence, Deposit money banks should prioritize the development and implementation of robust transparency policies. Deposit money banks should actively encourage visible utilization of information in various aspects of their banking services. Deposit money banks should establish and maintain robust collaborative efforts with relevant stakeholders so as to enhance information accountability within the banking sector.*

Keywords: *Information Accountability, Transparency, Visibility, Collaboration, Access Control, Innovative & Adaptability.*

Introduction

According to Samarati and Capitani (2001), access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. Access control protects against malicious attacks to privacy, authenticity and availability of the system. Computer security and the associated subjects have been, and continue to be, the biggest issue in the IT (Information technology) world. Access control has continued to adapt to growing IT-system applications. Access control was initially developed in multi-user and multi-level protected systems to protect sensitive data. This is to avoid unauthorized usage by unlawful users of machine resources and protect legal use the resources of the system (Lu, Gu & Xia, 2019). Access control is intended to monitor technical and technological tools in order to avoid unauthorized (confidential) and improper disclosure of malicious (integrity) changes, thus preserving access to controlled (availability) entities

According to Alhwait *et al.* (2020), access control is defined as an essential security requirement in the IT sector. Organizations has its own information management system that determines a

collection of policies based on circumstances where customers are able to access all or some of the program's resources. In other to achieve these resources; security policies are important. Access control focuses on authentication and potency, password-based securities, potentialities and access control list (ACLs), multilateral and multi-level securities, preventive control as well as networks are transformed, advanced disclosure system (IDS) and firewall controversy. In the side of network security, access control is the ability to restrict and monitor access across communication links to host systems and applications. To do this, any person that attempts to obtain access must first be detected, or authenticated, so that access rights can be personalized to the individual (Bhatti et al, 2019). Generally speaking, there are many aims of access control to protect objects (resources) of the computer system: Do not allow unauthorized users to access resources, prevents legal users from unauthorized access to services, allow legitimate users to have allowed access to resources, subjects, objects, freedom of access and authentication, permission, audits. These measures are needed so that the safety and unauthorized access to organizational resources can be guaranteed. That is why employees as well as organizations are required to be able to adapt swiftly to these technological needs as well as the need to become innovative, so that completive advantaged can be sustained.

For too long, our approach to information protection policy has been to seek ways to prevent information from "escaping" beyond appropriate boundaries, then wring our hands when it inevitably does. This hide-it-or-lose-it perspective dominates technical and public-policy approaches to fundamental social questions of online privacy, copyright, and surveillance. Yet it is increasingly inadequate for a connected world where information is easily copied and aggregated and automated correlations and inferences across multiple databases uncover information even when it is not revealed explicitly. As an alternative, accountability must become a primary means through which society addresses appropriate use.

Information accountability means the use of information should be transparent so it is possible to determine whether a particular use is appropriate under a given set of rules and that the system enables individuals and institutions to be held accountable for misuse. Transparency and accountability make bad acts visible to all concerned. However, visibility alone does not guarantee compliance. Then again, the vast majority of legal and social rules that form the fabric of our societies are not enforced perfectly or automatically, yet somehow most of us still manage to follow most of them most of the time. We do so because social systems built up over thousands of years encourage us, often making compliance easier than violation. For those rare cases where rules are broken, we are all aware that we may be held accountable through a process that looks back through the records of our actions and assesses them against the rules.

Personal privacy, copyright protection, and government surveillance are among the more intractable policy challenges in our information society. In each of these policy areas, excessive reliance on secrecy and up-front control over information has yielded policies that fail to meet social needs, as well as technologies that stifle information flow without actually resolving the problems for which they were designed. Information privacy rights aim to safeguard individual autonomy against the power that institutions or individuals gain over others through the use of personal information. Sensitive, and possibly inaccurate, information may be used against people

in financial, political, employment, and health-care settings. In democratic societies, citizens' behaviour is unduly restrained if they fear they are being watched at every turn. They may deliberately avoid reading controversial material or feel inhibited from associating with certain communities and ideas for fear of adverse consequences.

Solove (2004) states that protecting privacy is more challenging than ever due to the proliferation of personal information on the Web and the increasing analytical power available to large institutions (and to everyone else) through Web search engines and other facilities. Access control and collection limits over a single instance of personal data are insufficient to guarantee the protection of privacy when either the same information is publicly available elsewhere on the Web or it is possible to infer private details to a high degree of accuracy from other information that itself is public (Samarati, 2001, Sweeney & Anonymity, 2003]. Worse, many privacy protections (such as lengthy online privacy- policy statements in health care and financial services) are mere fig leaves over the increasing exposure of our social and commercial interactions. In the case of publicly available personal information, people often intentionally make the data available, not always by accident. They may not intend for it to be used for every conceivable purpose but are willing for it to be public nonetheless. Good security allows you to achieve a primary goal of the e-business era: reaching a greater number of customers with enhanced products and services. Information accountability stresses the need for information users to be transparent considering the pivotal role that information plays in the life of organizations as well as in governance. Therefore, this study seeks to investigate information accountability and access control of deposit money banks in Port Harcourt.

PROBLEM

Information is an important organisational resource that is central to all organizational activities and operations. Often times, organizational information is characterized by all forms of sensitivity, as a result, caution is required so as not to compromise be it personal or organizational information. Information accountability is one of such measure that ensures that the use of information by users is transparent so that it is possible to ascertain whether a particular use is appropriate under a given set of rules and that the systems enables individuals or organizations to be held accountable for information misuse. It becomes a cause for concern when information whether personal or organizational is used in secrecy or without relevant rules and guidelines in place to regulate the use of information such information. Especially due to the proliferation of media spaces with all sort of information through the emergence of big data. It is also a problem when information users do not participate nor give feedbacks on information used. Hence, the need of stressing on the relevance of information accountability both at an organizational and individual levels. It is as a result of this that this study sought to investigate the relationship between information accountability and access control of deposit money banks in Port Harcourt, Rivers State.

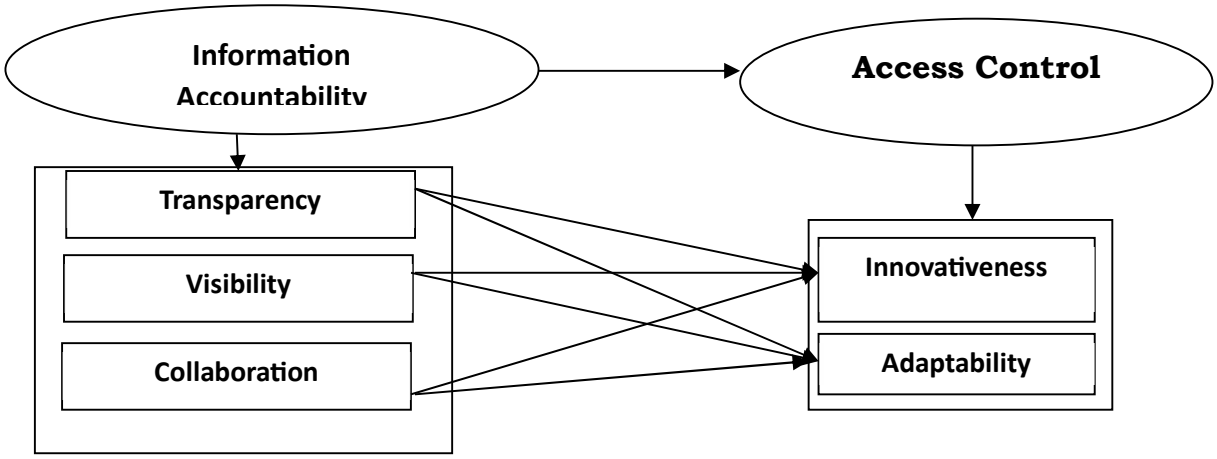

Fig.1.1: Conceptualisation of Information Accountability and Access Control

OBJECTIVES/QUESTIONS

The main objective of this research was to investigate the relationship between information accountability and access control of deposit money banks in Port Harcourt. In achieving the general objective, the study specifically explored;

- The role of transparency in enhancing access control of deposit money banks in Port Harcourt.
- How participation enhances access control of deposit money banks in Port Harcourt.
- The role of feedback mechanism in enhancing access control of deposit money banks in Port Harcourt.
- To what extent does transparency enhance access control of deposit money banks in Port Harcourt?
- How does participation enhance access control of deposit money banks in Port Harcourt?
- To what extent does feedback mechanism enhance access control of deposit money banks in Port Harcourt?

HYPOTHESES

In order to provide answers to research questions proposed earlier, the following hypothesis were formulated to guide the study;

H_{o1}: There is no significant relationship between transparency and innovativeness of deposit money banks in Port Harcourt.

H_{o2}: There is no significant relationship between transparency and adaptability of deposit money banks in Port Harcourt.

H_{o3}: There is no significant relationship between participation and innovativeness of deposit money banks in Port Harcourt.

H_{o4}: There is no significant relationship between participation and adaptability of deposit money banks in Port Harcourt.

H_{o5}: There is no significant relationship between feedback mechanism and innovativeness of deposit money banks in Port Harcourt.

H_{o6}: There is no significant relationship between feedback mechanism and adaptability of deposit money banks in Port Harcourt.

Theoretical Framework: Dynamic Capability Theory

The dynamic capability theory stresses on organizations ability to adapt in dynamic market conditions as a critical source of superior performance (Liu et al. 2012). Dynamic capability affirmed the firm's ability to recognize, integrate, develop, envisage, and reconfigure internal and external capabilities to deal with environmental dynamics (Pavlou & El Sawy, 2011). Literature argues that information accountability as a fundamental capability of an organization may influence on the dynamic capability and enhance the organizational performance (Cepeda & Vera 2007; Haas & Hansen 2005; Sher & Lee, 2004). KMO as a vital capability, provide an intellectual basis for organizations to respond for the internal and external contingencies (Ambrosini & Bowman, 2009).

Information Accountability

The information-accountability framework more closely mirrors the relationship between the law and human behaviour than do the various efforts to enforce policy compliance through access control over information. As an early illustration of information accountability at work today, consider credit bureaus and their vast collections of personal information. When these databases came on the scene in the consumer financial markets of the 1960s, policymakers recognized the public imperative to protect individual privacy and assure data accuracy, all while maintaining enough flexibility to allow analysis of consumer credit data based on the maximum amount of useful information possible. Under the Fair Credit Reporting Act (enacted 1970) (Alhwait et al, 2020), privacy is protected not by limiting the collection of data, but by placing strict rules on how the data may be used.

Analysis for the purpose of developing a credit score is essentially unconstrained, but the resulting information can be used only for credit or employment purposes. It cannot be used for marketing and other profiling. Strict penalties are imposed by the FCRA for the breach of these use limitations. Data quality is protected by giving all consumers the right to see the data held about them (transparency). If a user of the data makes a decision adverse to the consumer (such as denial of a loan or rejection of an employment application) the decision must be justified with reference to the specific data in the credit report on which the decision was based (accountability). If the consumer discovers that the data is inaccurate, he or she may demand that it be corrected. Stiff financial penalties are imposed by the FCRA against the credit bureau if it fails to make the appropriate corrections.

The typical consumer appreciates the paradox associated with protecting privacy and other information policy values through increased transparency. As the FCRA illustrates, we achieve greater information accountability only by making better use of the information that is collected and by retaining the data that is necessary to hold data users responsible for policy compliance. The success of this accountability regime for the past 40 years over a very large set of data-credit

reports on nearly every adult in the U.S. makes it a worthy model for considering policy compliance in other large systems.

Technical Architectures

Technical architecture is required to support information accountability by promoting accountability systems to build into our information infrastructures the technology necessary to make acts of information usage more transparent in order to hold the individuals and institutions who misuse it accountable for their acts. Systems supporting information accountability require three basic architectural features:

Policy-aware transaction logs. In a decentralized system each endpoint must assume the responsibility of recording information-use events that may be relevant to the assessment of accountability to some set of policies.

Policy-language framework. Assessing policy compliance over a set of transactions logged at a heterogeneous set of endpoints by diverse human actors requires a common framework for describing policy rules. Drawing on semantic Web techniques, larger and larger overlapping communities on the Web can develop shared policy vocabularies in a bottom-up fashion. A lack of perfect global interoperability of these policies is not a fatal flaw. Just as human societies learn to cope with overlapping and sometimes contradictory rules, so too are policy-aware systems likely to develop at least partial interoperability (Samarati & Capitani 2001).

Policy-reasoning tools. Accountable systems must be able to assist users in answering such questions as: Is this data allowed to be used for a given purpose? And can a given string of inferences be used in a given context, in light of the provenance of the data and the applicable rules? One possible approach to designing accountable systems is to place a series of accountable appliances throughout the system that communicate through Web-based protocols (Lunt, 2003). Accountability appliances would serve as proxies to data sources, mediating access to the data, and maintain provenance information and logs of data transfers. They could also present accountability reasoning in human-readable ways and allow annotation, editing, and publishing of the data and reasoning being presented (Kagal, Hanson, & Weitzner, 2008).

Elements of Information Accountability

Transparency

Physically, transparency is acknowledged as a materials' characteristic to conduct light. Due to this feature, things are easily observable through the mentioned substance. Whereas, transparency in social sciences is considered as the local authorities', companies', organizations' and individuals' operating characteristic, when activities, plans, funding and other significant information is provided publicly and clearly. Hence, both definitions of transparency emphasize the importance of visibility. In addition, the main aim is openness and communication, not confidence and concealment (Barth & Schipper, 2007). In this way, information disclosure can determine transparency and reliance on an entity (Wehmeier & Raaz, 2012).

Nevertheless, the opinion on transparency differs among various authors. For instance, Williams (2005) defines transparency using three features: relevant, timely and reliable information. Meanwhile Dubbink et al. (2008) exclude three transparency characteristics: effectiveness (positively associated with quality of information), freedom and virtue. Normally, transparency is related with organizations' public communication, ethics and reliance on it. Similarly, transparency is often described as conscientious communication, contrary to partiality,

advertisements and manipulation. Despite the variety of analysis aspects, the main attention in financial and social accounting or organizational researches is committed to information revelation, i.e. organization transparency depends on the publicly available information transparency. Therefore, transparency is generally acknowledged as the companies' financial and non-financial information accessibility for external users (Bushman et al., 2004). Hence, the transparency of business subjects' activities depends on the business information, i.e. financial and non-financial information, disclosure in financial and social responsibility statements, annual reports, Internet websites, communication channels, spread of information, etc.

Information Visibility

Visibility of information reflects whether or not the public can view program outputs. The public or groups can more easily hold the information users to be accountable when the program is more visible because of the ease of accessing information and monitoring outputs. For example, programs with readily visible outputs such as the development of a new school are more easily monitored than an education improvement program (Besley and Ghatak, 2003). In short, programs with visible outputs passively convey information to the public or groups about public sector performance. Observation the public or those saddled with the responsibility of regulating information use or groups may enhance accountability and program success in several ways. For example, observation may give rise to satisfaction or displeasure on the part of observers. This feedback can, in turn, prompt improvement in the implementation of the program.

Visibility may also lead to greater accountability in information use because it may help to create supportive constituencies (Wilson, 1989). Supportive constituencies can be particularly important in the implementation of reform programs where some users or influential individuals may try to block progress. Early, visible 'wins' that generate support for the overall program are therefore essential to sustain program implementation and bring it to completion (Barma, Huybens and Vin˜uela, 2014; Andrews, 2013). Holland (2017) also argues that using individuals' experiences with service provision helps to focus discussions between regulators and users. As services become more accessible, this can mean critical benefits for information accountability, leading to a virtuous cycle of visible information use, (Kilby, 2006; Holland, 2017).

Visibility has also been linked to information accountability through the mechanism of credit claiming. Visibility heightens the public profile of information users, motivating users to work towards openness, by avoiding misuse of information, and implement the program more effectively, so they can claim credit for, or at least be associated with, a successful program (Batley and Harris, 2014; Batley and Mcloughlin, 2015). More specifically, visibility makes it appealing for information users to forgo the benefits of corruption and program capture for the reputational benefits that this positive association will provide. While program visibility is to a large extent dictated by the type of program or policy involved (Lowi, 1964), there are an increasing number of tools for information users to enhance opportunities to make their programs more visible to the public. The constant development of information and communications technology has enabled the sharing of experiences, which can magnify the role of visibility for accountability. For example, Pakistan tried to harness the power of visibility, utilising an SMS platform to gather information on bribes from people who used public services. As of November 2014, 110,000 citizens had reported corruption issues out of the 500,000 who

responded to the SMS, and authorities took 3,600 actions against complaints (Marin, 2016; Verdenicci and Hough, 2015). Given this discussion, we expect public sector programs with greater visibility will see higher rates of success. When citizens and groups can more easily view progress of and outcomes from a program, they can then take actions that hold the government accountable for any number of program problems such as incomplete implementation, resource diversion or political interference.

Collaboration

Collaboration with relevant stakeholders or civil society groups in both private and public sector programs provides another type of opportunity for information accountability. Not only does collaboration offer potential for enhanced information-sharing mechanisms that are key to visibility and transparency, but collaboration also facilitates repeated two-way exchanges of information whereby information from principals (citizens or groups) can be conveyed directly to agents. Civil society organizations (CSOs) are particularly well positioned to demand accountability because of their greater organisational capacity, influence and resources compared to individuals (Sugiyama, 2016). Without organisation, citizens struggle to influence the policy process above their local government, and many decisions and acts of corruption occur above that level (Fox, 2015; Fox and Halloran, 2016; Brett, 2003; Fox and Aceron, 2016). Their ability to facilitate collective action is likely to make monitoring opportunities more valuable (Bauhr and Grimes, 2014), and some have even argued that transparency is only useful when combined with vehicles of collective actions (Fox, 2015; Cucciniello, Porumbescu and Grimmelikhuijsen, 2017). As such, collaboration with civil society organisations enables citizens to better use government information and more effectively work together to hold the government accountable.

CSOs have a number of avenues through which they can influence accountability and program success. First, they can help citizens access and decipher complex government documents. Second, CSOs amplify the collective voice of individuals. When CSOs draw attention to misdeeds of bureaucrats and spread information, monitoring has been found to be more effective (Sugiyama, 2016; Lindberg, Luehrmann and Mechkova, 2017). Third, they can aggregate demands from citizens and ensure they are coherent (Ackerman, 2005). This suggests that when CSOs collaborate with government in program development, they can present individuals voices in a more focused manner. Collaboration between government and CSOs in the implementation of public sector programs has been found to lead to success in diverse contexts. In one study of World Bank projects, for example, increasing the number of non-state actors participating in the project leads to overall improvements in project outcomes (Shin, Kim and Sohn, 2017, Bestaman & Nwanko, 2022) also stresses on the relevance of collaboration, when they stated that; collaboration leads to organisational success.

Concept of Access Control

One of the basic concepts of protection models is access control. The purpose of access control to data in information system is a limitation of actions or operations that the system's users can execute. The access control based on role concept represents interesting alternative in relation to traditional systems of DAC (Discretionary Access Control) type or MAC (Mandatory Access

Control) type. RBAC (Role-Based Access Control) model based on a role concept defines the user's access to information basing on activities that the user can perform in a system.

Robertson (2005) affirms that security policies of information systems determine that it is necessary to define for each user a set of operations that it could be perform. Due to it the set of permissions should be defined for each system's user. It suffices to determine the permissions for execution of particular methods on each object accessible for that user. It is exists the need to create the tool, designated mainly for security administrator who could manage one of the security aspects of information systems, namely the control of users' access to data stored in a system. To create the administration tool the access control model based on role concept in extended version (extended RABC) was chosen. It is necessary to deliver the tool allowing the definition of access control rules for any information system. It is exists the need to ensure the integrity of defined early access control rules in situation when we want to extend the existing information system by new components (i.e. applications). It is also necessary take the attention that two actors were distinguished in the design process of an information system and its associated security scheme: application/system developer and security administrator who cooperate with each other to define and apply the set of roles defined for particular system's users in according with security constraints assuring the global security strategy of an enterprise.

Robertson (2005) posited that access control represents one of the components of information system security, named logical security. Logical security contains three mutually supportive technologies that can be used to provide the system security: authentication, access control and audit. However, access control is the most important technique on logical security level and it is used frequently. Access control allows defining the user's responsibilities and possibilities in a system. It can define what a user can do directly and also what programs executing on behalf of the user are allowed to do. Access control limits the activities of successfully authenticated users basing on the security constraints defined on the conception level and on the administration level. An important requirement of any information management system is to protect data and resources against unauthorized disclosure (secrecy) and unauthorized or improper modifications (integrity), while at the same time ensuring their availability to legitimate users (no denials-of-service). Enforcing protection therefore requires that every access to a system and its resources be controlled and that all and only authorized accesses can take place. This process goes under the name of access control. The development of an access control system requires the definition of the regulations according to which access is to be controlled and their implementation as functions executable by a computer system.

Innovativeness

Innovation is a concept with a very large applicability, whose characteristics vary based on the field of reference. According to the National Institute of Statistics (2013), innovation is an activity resulting in a new product (goods or services) or a significantly improved one, a new process or a significantly improved one, a new marketing method or a new organizational method. Glodeanu et al. (2009) quoted the definition of innovation established by the European Union as" an accomplishment of a new idea in the current direct practice, either in a commercial manner, or in a voluntary and public sphere", by" the diffusion, assimilation and the usage of invention in different fields of the society". They continued by adding that it is accomplished either by" the

transfer of existing knowledge from one field to other fields (the leverage strategy)", by" using existing knowledge to redefine what is already known (the expansion strategy)", by" creating a new field of knowledge (the accomplishment strategy)", or by" creating a new field of knowledge around a vision or a vague idea on a future field of knowledge (the experimental strategy)" (Glodeanu et al., 2009). The latter one is the fundament of radical innovation, ensuring thus the break from the existing models. Innovation is production or adoption, assimilation, and exploitation of a value-added novelty in economic and social spheres; renewal and enlargement of products, services, and markets; development of new methods of production; and establishment of new management systems; it is both a process and an outcome" (Crossan & Apaydin, 2010).

Adaptability

Adaptability is the ability of an organization to recognize the need to change and seize opportunities in dynamic environments. In an increasingly complex world, leadership must pay close attention to dynamic, distributed, and contextual aspects in order to position their organizations for adaptability. The theory of dynamic capabilities constitutes a central concept for the requirements that enable organizational adaptability. According to (Uhl-Bien & Arena 2018), Adaptation to changing environmental conditions is a focal subject of organizational studies and deemed a necessity for organizations in every industry. The dynamic nature of most competitive environments requires organizations to continuously or periodically innovate in order to create a competitive advantage and eventually to survive (Hauschildt et al. 2016).

Furthermore, Wiltbank et al. (2006) highlighted the significant empirical support for adaptive organizations having higher chances to succeed; in his words, flexible and adaptive organizations are able to outmanoeuvre their competitors by quickly capturing new opportunities. This can ultimately lead to improvements in the competitive position of an organization and increase the organization's performance. A central concept capturing the notion of the need for organizations to change is organizational adaptability, which (Birkinshaw & Gibson, 2004) defined as "the ability to move quickly towards new opportunities, to adjust to volatile markets and to avoid complacency". Among the many theories that were established covering organizational change, a common parameter of all theories is that change is oriented towards a specific individual goal (van de Ven & Poole 2005).

Methods

The study population embraced 80 principal officers of deposit money banks in Port Harcourt, since the study was measuring access control of deposit money banks. Four managers were randomly selected from 20 deposit money banks in Port Harcourt, giving us a total population of 80 respondents which also serves as the sample, due to the focus of the study. A cross sectional survey strategy was adopted for the study. The content validity of the instrument was established by giving a set of the drafted questionnaire to four managers occupying leadership positions in their organizations and four questionnaires to other researchers in the specific area of executive decision-making. These executives reviewed the content of the instrument and confirmed that the items were suitable for gathering relevant data for the research study.

Data Analysis

To empirically evaluate the relationship between the predictor and criterion variables of this study (including their dimensions and measures), the spearman's rank order of correlation coefficient (RHO) was employed. As a tool, it is considered to be more flexible and it is not limited or confined to parameters statistical assumption such as applicable in the Pearson's product moment correlation. The analysis was done using the scientific package for social sciences (SPSS) version 23 software. We begin by showing evidence of a relationship between the variables.

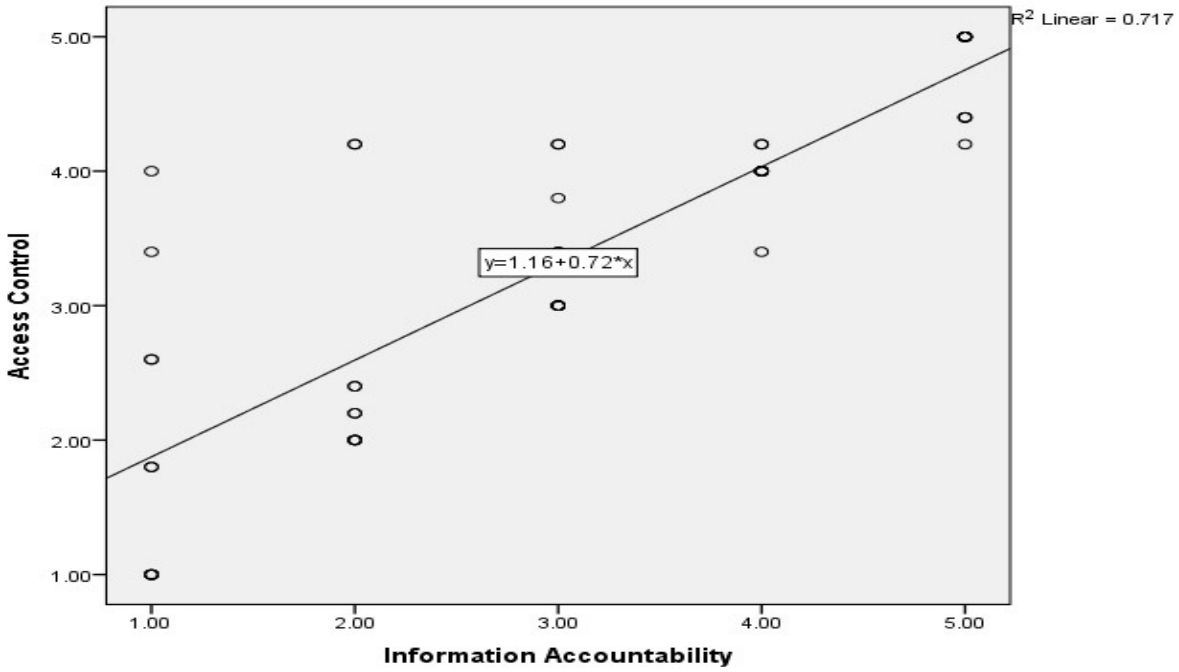

Figure 1: Scatter plot for information accountability and access control

Figure 1 shows a strong relationship between information accountability (independent variable) and access control (dependent variable). The scatter plot graph shows that the linear value of (0.717) depicting a very strong viable and positive relationship between the two constructs. The implication is that an increase in information accountability simultaneously brings about an increase in the level of access control. The scatter diagram has provided vivid evaluation of the closeness of the relationship among the pairs of variables through the nature of their concentration.

Table 1: Correlation for Transparency and Access Control Measures

			Transparency	Innovativeness	Adaptability
Spearman's rho	Transparency	Correlation Coefficient	1.000	.818**	.768**
		Sig. (2-tailed)	.	.000	.000
		N	68	68	68
	Innovativeness	Correlation Coefficient	.818**	1.000	.898**
		Sig. (2-tailed)	.000	.	.000
		N	68	68	68
	Adaptability	Correlation Coefficient	.768**	.898**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	68	68	68

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

Source: SPSS Output

Ho_1: There is no significant relationship between transparency and innovativeness of deposit money banks in Port Harcourt.

Table 1 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.818 on the relationship between transparency and innovativeness. This value implies that a very strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in innovativeness was as a result of the transparency. Table 1 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between transparency and innovativeness of deposit money banks in Port Harcourt.

Ho_2: There is no significant relationship between transparency and adaptability of deposit money banks in Port Harcourt.

Table 1 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.768 on the relationship between transparency and adaptability. This value implies that a strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in adaptability was as a result of the transparency. Table 1 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between transparency and adaptability of deposit money banks in Port Harcourt.

Table 2: Correlation for Visibility and Access Control Measures

			Visibility	Innovativeness	Adaptability
Spearman's rho	Visibility	Correlation Coefficient	1.000	.852**	.775**
		Sig. (2-tailed)	.	.000	.000
		N	68	68	68
	Innovativeness	Correlation Coefficient	.852**	1.000	.898**
		Sig. (2-tailed)	.000	.	.000
		N	68	68	68
	Adaptability	Correlation Coefficient	.775**	.898**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	68	68	68

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

Source: SPSS Output

Ho_3: There is no significant relationship between visibility and innovativeness of deposit money banks in Port Harcourt.

Table 2 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.852 on the relationship between visibility and innovativeness. This value implies that a very strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in innovativeness was as a result of the visibility. Table 2 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between visibility and innovativeness of deposit money banks in Port Harcourt.

Ho_4: There is no significant relationship between visibility and adaptability of deposit money banks in Port Harcourt.

Table 2 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.775 on the relationship between visibility and adaptability. This value implies that a very strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in adaptability was as a result of the visibility. Table 2 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between visibility and adaptability of deposit money banks in Port Harcourt.

Table 3: Correlations for Feedback Mechanism and Access Control Measures

			Collaboration	Innovativeness	Adaptability
Spearman's rho	Collaboration	Correlation Coefficient	1.000	.752**	.710**
		Sig. (2-tailed)	.	.000	.000
		N	68	68	68
	Innovativeness	Correlation Coefficient	.752**	1.000	.898**
		Sig. (2-tailed)	.000	.	.000
		N	68	68	68
	Adaptability	Correlation Coefficient	.710**	.898**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	68	68	68

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

Source: SPSS Output

Ho_5: There is no significant relationship between collaboration and innovativeness of deposit money banks in Port Harcourt.

Table 3 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.752 on the relationship between collaboration and innovativeness. This value implies that a very strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in innovativeness was as a result of the collaboration. Table 3 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between collaboration and innovativeness of deposit money banks in Port Harcourt.

Ho_6: There is no significant relationship between visibility and adaptability of deposit money banks in Port Harcourt.

Table 3 shows a Spearman Rank Order Correlation Coefficient (rho) of 0.710 on the relationship between visibility and adaptability. This value implies that a strong relationship exists between the variables. The direction of the relationship indicates that the correlation is positive; implying that an increase in adaptability was as a result of the visibility. Table 3 also shows the statistical test of significance (p-value) which makes possible the generalization of our findings to the study population. From the result obtained the sig- calculated is less than significant level ($p = 0.000 < 0.05$). Therefore, based on this finding the null hypothesis earlier stated is hereby rejected and the alternate upheld. Thus, there is a significant relationship between visibility and adaptability of deposit money banks in Port Harcourt.

Presentation

The result revealed that there is a positive and significant relationship between information accountability and access control of deposit money banks in Port Harcourt. Iinformation accountability in deposit money banks is a crucial aspect of ensuring transparency and trust in the financial system. According to Emmanuel et al. (2017), information accountability refers to the responsibility of deposit money banks to provide accurate and reliable information to stakeholders, including customers, regulators, and shareholders. In an era where data breaches and fraudulent activities are on the rise, it is imperative for banks to establish robust mechanisms for information accountability. This involves implementing strict data protection and security measures to safeguard customer data, as well as ensuring that financial reports and disclosures are accurate and timely. In today's digital age, where information is increasingly vulnerable to cyber threats, the concept of information accountability becomes even more pertinent. It requires banks to proactively address potential risks and take necessary measures to protect sensitive information from unauthorized access. Furthermore, information accountability also extends to the ethical use of customer data, as banks must adhere to privacy regulations and guidelines when collecting, storing, and sharing personal information. By upholding the principles of information accountability, deposit money banks can not only safeguard their reputation but also contribute to the overall stability and confidence in the financial sector.

Access control is of utmost importance in Port Harcourt's deposit money banks due to several reasons. Firstly, effective access control systems ensure the protection of sensitive information and assets within the banks. As highlighted by Nwinyokpugi and Omunakwe (2019), access control mechanisms such as biometric authentication and card-based systems help prevent unauthorized individuals from gaining entry into restricted areas, thus safeguarding valuable assets and confidential data. Secondly, access control plays a crucial role in maintaining the privacy and confidentiality of customer information. The banking sector deals with a vast amount of personal and financial data, including account details, transaction history, and identification documents. By implementing access control measures, banks can restrict access to this information, ensuring that only authorized personnel can handle and view customer data. Moreover, access control systems enable banks to monitor and track employee activities, which is essential in detecting and preventing internal fraud or misconduct. By implementing access control measures, banks can limit access to critical systems and monitor employee actions, thus reducing the potential for unauthorized activities within the organization (Nwinyokpugi & Omunakwe, 2019). Overall, the implementation of robust access control systems in Port Harcourt's deposit money banks is crucial to protecting valuable assets, maintaining customer privacy, and mitigating internal risks. (Nwinyokpugi and Omunakwe, 2019). A robust access control system provides the necessary foundation for ensuring information accountability in deposit money banks. By implementing access control measures, such as user authentication, role-based access control, and audit trails, deposit money banks can effectively enforce information accountability and mitigate the risk of data breaches or unauthorized access to sensitive information. Therefore, the positive relationship between information accountability and access control is crucial in maintaining the security and integrity of customer data in the banking sector.

Conclusion and Recommendation

The study concludes that information accountability positively enhances access control of deposit money banks in Port Harcourt. This implies that when deposit money banks implement robust accountability measures, it positively influences their ability to control access to sensitive information. This correlation highlights the crucial role of information accountability in enhancing the security and confidentiality of data within the banking sector.

Therefore, based on the foregoing conclusion, the following recommendations were made:

i. Deposit money banks should prioritize the development and implementation of robust transparency policies. These policies should outline the principles and guidelines for disclosing relevant information to customers, regulators, and other stakeholders. Transparent communication fosters trust and confidence in the banking system and helps customers make well-informed decisions.

ii. Deposit money banks should actively encourage customer visibility of information use in various aspects of their banking services. This includes seeking feedback through surveys, suggestion boxes, or online feedback forms. By involving customers in decision-making processes, banks can better understand their needs and preferences, leading to improved access control mechanisms tailored to customer.

iii. Deposit money banks should engage in collaborative efforts with relevant stakeholders so as to boost the quest for information accountability in the banking industry and beyond.

References

Ackerman, J. M. (2005). Social Accountability in the Public Sector: A Conceptual Discussion (Paper No. 82). The World Bank. Retrieved http://documents.worldbank.org/curated/en/514581468134386783/pdf/357330Ackerman.pdf.

Alhwaiti, A. K., Leider, A. & Tappert, C. (2020). Advances in Information and Communication, vol. 70, no. January. Springer International Publishing.

Ambrosini, V., and Bowman, C. (2009). What are dynamic capabilities and are they a useful construct in strategic management.

Bauhr, M. & Grimes, M. (2014). Indignation or Resignation: The Implications of Transparency for Societal Accountability. Governance 27:291–320. doi:10.1111/gove.12033

Batley, R. & Harris, D. (2014). Analysing the Politics of Public Services: A Service Characteristics Approach. Overseas Development Institute. Retrieved https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/8913.pdf.

Barma, N. H., Huybens, E., Vin˜uela, L. (2014). Institutions Taking Root: Building State Capacity in Challenging Contexts. Washington, DC: World Bank Publications.

Barth, M. E., & Schipper, K. (2007). Financial Reporting Transparency. Journal of Accounting, Auditing & Finance, 23, 173-190.

Bestman, E. A. & Nwankwo, V. O. (2023). Corporate Learning and Employee Development. Unpublished Masters Dissertation in Rivers State University.

Bhatti, M., Samejo, A. & Danwar, S. (2019). "A Review of Security Levels of Data Encryption Algorithms. 4(3), 31–35

Besley, T. & Ghatak, M. (2003). Incentives, Choice, and Accountability in the Provision of Public services. Oxford Review of Economic Policy 19:235–249. doi:10.1093/oxrep/19.2.235.

Bonino F., with Jean, I. and Knox Clarke, P., ALNAP/ODI. (2014) Closing the Loop - Practitioner guidance on effective feedback mechanisms in humanitarian contexts. www.alnap.org/help-library/closing-the-loop-effective-feedback-in-humanitarian-contexts

Bushman, R., Piotroski, J., & Smith, A. (2004). What Determines Corporate Transparency? Journal of Accounting Research, 42, 207-252.

Cepeda, G., and Vera, D. (2007). Dynamic capabilities and operational capabilities: A knowledge management perspective. Journal of Business Research, 60(5), 426-437.

Crossan, M. M., and Apaydin, M. (2010). A Multi-Dimensional Framework of Organizational Innovation: A Systematic Review of the Literature. Journal of Management Studies, 47(6), 1154-1191.

Cucciniello, M., Porumbescu, G. A., & and Grimmelikhuijsen, S. (2017). 25 Years of Transparency Research: Evidence and Future Directions. Public Administration Review 77:32–44. doi:10.1111/puar.12685.

Dubbink, W., Graafland, J., & van Liedekerke, L. (2008). CSR, Transparency and the Role of Intermediate Organisations. Journal of Business Ethics, 82, 391-406.

Fox, J. A. (2015). Social Accountability: What Does the Evidence Really Say? World Development 72:346–361. doi:10.1016/j.worlddev.2015.03.011.

Glodeanu, I., Hoffman, O., Leovaridis. C., Nica, E., Nicolaescu, A., Popescu, G., and Rașeev, S. (2009). New paradigms of innovation. Case study – the corporate university. Bucharest: Expert Publishing House.

Haas, M. R., & Hansen, M. T. (2005). When using knowledge can hurt performance: The value of organizational capabilities in a management consulting company, Strategic Management Journal, 26(1), 1-24.

Hauschildt, Jürgen, Sören Salomo, Carsten Schultz, and Alexander Kock. (2016). Innovations management, 6th ed. Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften. München: Franz Vahlen.

Holland, J. (2017, June). What Works for Social Accountability? Findings from DFIDs Macro Evaluation. (Policy Briefing). Department for International Development. Retrieved https://gpsaknowledge.org/knowledge-repository/what-works-for-social-accountability-findings-from-dfids-macro-evaluation/.

Kagal, L., Hanson, C., & Weitzner, D. (2008). Integrated policy explanations via dependency tracking. In Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks.

Lindberg, S. I., Luehrmann, A., & Mechkova, V. (2017). From De-jure to De-facto: Mapping Dimensions and Sequences of Accountability. (Background Paper to World Development Report). The World Bank. Retrieved http://documents.worldbank.org/curated/en/324501487592445304/pdf/112920-WP-PUBLIC-WDR17BPAccountabilitypaper.pdf.

Liu, Z., Gu, W. & Xia, J. (2019). "Review of Access Control Model," Comput. Mater. Contin., 61(3), 43–50. doi: 10.32604/jcs.2019.06070.

Liu, H., Ke, W., Wei, K. K. & Hua, Z. (2012). The impact of IT capabilities on firm performance: The mediating roles of absorptive capacity and supply chain agility. Decision Support Systems, 54(3), 1452-1462.

Lowi, T. J. (1964). American Business, Public Policy, Case-Studies, and Political Theory. World Politics 16:677–715. doi:10.4324/9781315125992-11.

Lunt, T. Protecting Privacy in Terrorist-Tracking Applications. Presentation to the Department of Defense Technology and Privacy Advisory Committee (Washington, D.C., Sept. 29, 2003).

Marin, J. M. (2016). Evidence of Citizen Engagement Impact in Promoting Good Governance and Anti-Corruption Efforts. (U4 Expert Answer No. 21). Transparency International. Retrieved https://www.u4.no/publications/evidence-of-citizen-engagement-impact-in-promoting-good-governance-and-anti-corruption-efforts.pdf.

National Institute of Statistics (2013). Romania Statistical Yearbook 2012. http://www.insse.ro/cms/files/Anuar%20statistic/13/13.Stiinta,%20tehnologie%20si%20inovare_ro.pdf.

Pavlou, P. A., & El Sawy, O. A. (2011). Understanding the Elusive Black Box of Dynamic Capabilities. Decision Sciences, 42(1), 239-273.

Robertson, J. (2005). Principles of effective information management. Step Two Design pty Limited.

Samarati, P. & De Capitani, S. (2001). "Access Control: Policies, Models.

Samarati, P. (2001). Protecting respondent's privacy in microdata release. IEEE Transactions on Knowledge and Data Engineering 13(6), 1010–1027.

Solove, D. (2004). The Digital Person. New York University Press, New York,

Sher, P. J., and Lee, V. C. (2004). Information technology as a facilitator for enhancing dynamic capabilities through knowledge management, Information & Management, 41(8), 933-945.

Shin, W., Kim, Y., & Sohn, H. (2017). Do Different Implementing Partnerships Lead to Different Project Outcomes? Evidence from the World Bank Project-Level Evaluation Data. World Development 95:268–284. doi: 10.1016/j.worlddev.2017.02.033.

Sugiyama, N. B. (2016). Pathways to Citizen Accountability: Brazil's Bolsa Familia. The Journal of Development Studies 52:1192–1206. doi: 10.1080/00220388.2015.1134779.

Sweeney, L. & K-anonymity (2002). A model for protecting privacy. International Journal on Uncertainty, Fuzziness, and Knowledge-based Systems 10(5), 687–570.

Uhl-Bien, Mary, and Michael Arena. (2018). Leadership for organizational adaptability: A theoretical synthesis and integrative framework. The Leadership Quarterly 29: 89–104.

Van de Ven, Andrew H., and Marshall Scott Poole. (2005). Explaining Development and Change in Organizations. Academy of Management Review 20: 510.

Verdenicci, S. & Hough, D. (2015). People, Power, and Anti-Corruption: Demystifying Citizen-Centred Approaches. Crime, Law and Social Change 64(1):23–35. Retrievedhttp://sro.sussex.ac.uk/id/eprint/56890/8/CLSC%252C_Article%252C_20_Apr_15.pdf.

Wehmeier, S., & Raaz, O. (2012). Transparency matters. The concept of organizational transparency in the academic discourse. Public relation inquiry, 1, 337–366.

Wiltbank, Robert, Nicholas Dew, Stuart Read, and Saras D. Sarasvathy. (2006). What to do next? The case for non-predictive strategy. Strategic Management Journal (27), 981–98.

Williams, C. C. (2005). Trust diffusion: the effect of interpersonal trust on structure, function and organizational transparency. Business and Society, 44, 357-368.