American International Journal of Business Management (AIJBM)
ISSN- 2379-106X, www.aijbm.com Volume 8, Issue 5 (May - 2025), PP 63-73

A Study on Data Protection and Information Management in Financial Institutions in Sierra Leone

Oludolapo O. Akinyosoye–Gbonda (Ph.D.)
Alhaji Y. Kenneh (Ph.D. Candidate)
Mohamed S. Conteh
Institute of Public Administration and Management – University of Sierra Leone

ABSTRACT:- Data protection is ensuring sensitive data such as financial information are accessed only by authorised personnel while information management refers to a systematic process of collecting, organising, retrieving, analysing and disseminating information within or out of an organisation. This study seeks to examine the significance of data protection and information management; how it affects and contributes to the operations of a commercial bank in Sierra Leone and to provide solutions to its challenges. A well-structured and validated questionnaire was administered to 50 staff randomly selected from junior and senior categories of staff from different departments in a commercial bank. Data obtained from the field survey were analyzed and presented using statistical tools. The study revealed that data protection and information management have led to the transformation of R Commercial Bank in order to achieve its primary financial objectives. Also, the bank has encountered numerous problems that have posed a threat to data security and information management as a result of ineffective policy implementation. To address the threat of insecurity, proper measures of policy adherence had to be enforced. The researchers recommend that the R Commercial Bank should minimise the quantity of data collection, only necessary data must be collected; embark on data encryption; enforce strict data protection and information management policy and enforce strict monitoring of data usage.

Keywords:- Data Protection, Information Management, Commercial Bank, Data Security and Data encryption.

I. INTRODUCTION

Data protection and information management in financial institutions in Sierra Leone is one of the most important components in day to day running of business administration and financial management. It is very important for banks and other financial institutions to have made tremendous progress in achieving their primary objectives but there has been an ongoing challenge that has continued to be a threat to the banking sector and financial institutions. In this context data can be defined as any information that has not been processed, define, edited, analyses and fit for purpose, in general it is some set of characters that is gathered and translated for a particular purpose, usually analysis. This study will examine the case of the R Commercial Bank of Sierra Leone.

This study will assess how the R Commercial Bank protects its data and manages information. The goal of the study is to understand how important this is for banking operations and identify any obstacles that make it difficult. In the past few years, keeping customer information safe in banks has been a big issue. It has caused problems with how information is managed in the R Commercial Bank. So, based on the findings of this study, the researcher will proffer important recommendations to help solve the problem. the R Commercial Bank was established in 1971 with 100% of its shares owned by the parent company. In 1973, the government of Sierra Leone owned about 25% shares in the Bank and later that same year. The Bank has sixteen (16) branches across the country.

The R Commercial Bank has been one of the leading financial institutions that contributed towards sustainable national development through loan scheme programs, for local investment, provision of financial management services to the public, employment, and the implementation of financial policies through the Central Bank of Sierra Leone. Data protection and information management in financial institutions has over the years become a fundamental principle for the R Commercial Bank, because of the robust integration of information and communication technology into the banking operations.

As one of the oldest financial institutions that have maintained effectiveness and consistency in public service delivery, it has been faced with the need to transition into the revolution to integrate artificial intelligence that requires the use of high-tech systems in the day-to-day banking operations across the country.

With the rapid evolution of information and communication technologies, it has assumed central importance in the organizational function and structure of all departments in the institution.

In the late 90s, the country experienced the emergence of foreign Banks into the country with different banking systems, marketing strategies, management tactics, and a modernized banking system that required the use of information and communication technology. This emergency, however, forced the R Commercial Bank and other financial institutions to integrate the use of advanced technology to rise to the occasion. Early 2000 saw a new era of competitiveness among banking institutions across the country, and data management became a reliable asset that serve as a source of information, education, and innovation that led to the pinnacle of excellence amongst other Banks. Data protection and management have been a key component of the bank in recent years.

Marchi, L. (2003), defines data as a presentation of facts, concepts or instructions in a formalized manner which should be suitable for communication, interpretation, or processing by human or electronic machine. Data management and security in the banking sector and any other financial institution requires the use of advance technological equipment, knowledge and adequate resources. Some banks among many other local banking institutions have been able to gain competitive edge in the banking industry due to their information management systems, online services, data policies and regulations, financial management system that is in line with the international standard. In view of this, banks have been very proactive in dealing with growing challenges on the transformation of the electronic banking system. In response to the ongoing threat of data breaches, identity theft, hacking, and similar fraud across banking and financial institutions are consistent and effective in enhancing data privacy programs. Data management and protection is very key to the reputation of banks, success and achievement. Therefore, it is important to note that data protection and management comes with great advantages and added value to operation of banks. In recent years, some banks have been striving and competing for awards such as being - the most reliable financial institutions and have been gaining competitive edge in their banking operations while others try to trail behind in Sierra Leone. However, this endeavour come with huge cost though they have made tremendous gain in their approach to data management and security.

Other areas of achievements in recent years include: i. customers' satisfaction - it is an obvious fact that customer satisfaction is derive based on the good performance of staff, quality information management system, and confidentiality of customers detail information. It is therefore, imperative for financial institutions like the banks for instance, to have a comprehensive data privacy program; ii. Increase in revenue generation - the policies implemented by these banks in response to data protection and management have completely helped to expand the operations of the bank across the country. However, these banks have made an increment of at least 39% in its revenue generation according to its annual report. Due to its online banking systems, they have attracted more customers beyond the borders of Sierra Leone; iii. increase knowledge in information system – these banks are determined to ensure that they provide their customers and the public quality service delivery to enhance customers' satisfaction and set the standards for banking operations in Sierra Leone. They have over the past years engaged in staff training on information communication programs. This has exposed most of their staffs to the use of advance technological equipment's, and software; iv. Financial security - major banks in Sierra Leone send texts to customers on their mobile phones to alert them about large purchases or unusual account activity debit and credit messages. Most of the local and international banks in Sierra Leone are now trying to convert their customers' smartphones into security tokens so that it can provide them with added layer of protection. Technological innovations in the banking sector and financial institutions in Sierra Leone have greatly increased the capacity of financial services providers to capture, store combine and analyses a wide variety of customers' data, such as their financial situation, habits, preferences, and physical location. However, these trends can bring more advantages to customers but comes with new risks specific to the financial services sector may require a comprehensive policy response. Positive outcomes of data management systems may include potentially cheaper and more relevant financial products and access to credit for those without any traditional credit record. On the other hand, customers may not be aware of the extent to which their data is being used. For instance, customers may risk marginalization as a result of impervious and potentially unfair data mining practices, or find themselves exposed to fraud and cybercrime. Data management and protection in the banking industry is a major concern for all stakeholders' society i.e. the customers, policy makers, management, the government and the general public, Andrew P.C. Stephens (2019).

Regardless, of the progress and achievement made by financial institutions in terms of data protection and information management, there have been numerous challenges and setback that have limited data protection and information management in Sierra Leone. Data breach and information leaks in financial institutions are a growing challenge that occurs every day and it has become a national concern for both the public and private sectors. The key problems that affect data protection and information management in

financial institutions are: i. Poor Data Management and Security - there have been a lot of problems that have posed a serious threat to data management and security. Internet and electricity supply have led to an increase in data problems. Banking institutions are built upon a strong system of internet connection and program applications that it cannot function without. In recent times some indigenous banks have been faced with losing billions of Leone due to the hacking of relevant information in their database systems; ii. Availability of a strong internet connection - Internet accessibility has been a major challenge for banking institutions to effectively function. The deployment and maintenance of computing systems, storage systems, and information management is a very big challenge because of poor internet facilities. For the past decades, several banks have shut down their operations due to poor data management system, electricity supply, and poor internet system; iii. Formulation and implementation of public financial policies - the government of Sierra Leone through the central bank and international and local banks are responsible to formulate and implement financial policies that can protect financial management and monetary transactions; iv. Human element security threats - This remains to be the number one major problem in data protection in the banking sector. The human element has been the cause of all attacks, hacking, and deleting of relevant information from the system and it is factual that the computer cannot operate on its own.

As with any other sector, banking has its ups and downs when it comes to risks and offers associated with sensitive personal, financial information alongside data protection regulations. One advantage is that customers can increase the amount of trust that they have against security breaches because regulation frameworks push institutions to adopt new technologies and invest in advanced frameworks to manage their data (Serrado et al, 2020).

II. MATERIALS AND METHODS

2.1 Review of Literature

As a matter of principle, the area of data protection and information management can be viewed from different scientific angles to understand the theory relevant to the research questions. This study sets out to explore the general data protection regulation in financial services industries grounded on the pivotal question: "How do companies approach General Data Protection Regulation and what can we learn from their approaches? Data privacy and information management has been a very key component for financial institutions all over the world. In response to address challenges that hinder the progress and achievement of these institutions the central bank of Sierra Leone for the past decades since the evolution of advance technology into the global market system and has been cascaded down to all institutions, Schumacher, L. (2013).

Information management system is a very broad concept to discuss with reference to financial management system in the banking sector and financial institutions, Baskerville, R. (2011). The publication of the institute for data management and information system in 2016 developed a theory that answer the questions on how data protection can be maintain as the threat continues to increase, Jegadeesan, H. (2014). It highlights the processes and procedures of how the institution should function within an enabling environment. The key features of information management system are data storage, data retrieval, data security and integrity, information access, and data processing, Schumacher, L. (2013).

Some financial institutions are faced with poor management system and the lack of coordinated system to facilitate the flow of communication and the protection of data within the organisational structure, Edwards, John. 2019. In financial institutions, data security and privacy is a fundamental feature to an efficient information management system. When there is a gap in communication, knowledge, performance and proper coordination, it objectively indicates that there is a weak system of information management, Balkin, Jack M. (2016). Banking and financial services industry should have a cyber-security department. This cyber security department deploy some of the common security measures in order to secure systems.

Therefore, financial policies and regulations critically examine and monitor financial transaction, trade and innovations whiles on the other hand some of the policies focuses on information management system, customers' right to access information, protection of customers' confidential information and financial security. For now, Sierra Leone has no data protection Act but the telecommunication Act No.9 of 2006, which regulate the telecom companies.

Information management system is a very broad concept to discuss with reference to financial management system in the banking sector and financial institutions, Baskerville, R. (2011). However, information management system can be referred to as a computer system or a set of programs that is used to track and store relevant information for organisational use. Most importantly, it can be used to track anything from financial data to inventory levels and customer information, Jun, M., & Cai, S. (2001). These systems are the backbone of any organisation to function efficiently and effectively. They help the managers, technical staff and middle management to manage information, data and knowledge in a structured way.

Business intelligence is a subset of these systems and helps the institution to make better decision by providing them with the insights from their data. It is important to note that information management system in the banking sector and financial institutions play a pivotal role to coordinate and defines the principles, value and standard of the institutions,

These security measures include Secured Socket Layers for secure connection, vulnerability and assessment testing of systems, database encryption, Firewalls to control flow of traffic, Intrusion detection systems, Network intrusion prevention systems, quarantining unknown systems, Domain Name systems, password protection mechanism and Short Message Service alerts to customers, Barrett, Lindsey. (2019). All of these devices and security systems are to secure cloud architecture infrastructure in the banking and financial services.

Alongside such enhancement frameworks as data filtering, data management goes a long way and can put the institution itself in an equally good position. This proactive approach to data governance not only protects customer information from breaches and misuse but also enhances the bank's reputation, a vital asset for attracting and retaining clients (Rodrigues et al, 2022). Regulations regarding data alongside the department of media and communication studies (DMCS) in Europe force financial organizations to adopt new technologies which compliment changes done in analytics and enhance digital capabilities (Luo, 2021) (Voglhofer & Rinderle-Ma, 2019). In trying to comply with legal guidelines, financial entities become less exposed to the risks related to legal fines or litigations concerning breaches of the organizational data or non-conformity clauses (Uzougbo et al, 2024) (Webster, 2017). When an individual is provided the legal authority to exercise jurisdiction over his/her neutral information, it implies that such person possesses the ability to give permission regarding the collection of such information and thus leads to (organizational purposes) using such private data without infringing the privacy (Biswal & Kulkarni, 2021).

2.1.1 Current Empirical Literature Relevant to the Research Questions

Desk review of journals, books, conference proceedings, and articles, published and unpublished materials from various institutions and the internet relevant sources to the study were adopted to underpin the study. Additionally, different writers have contended that, data protection. Moyo, T. & Mamobolo, M. 2014. Therefore, it was stated that to achieve this, there is a need to employ some key stakeholders into the implementation of public programs and information management in financial institution and the banking sector requires internet availability and proper storage system. According to Rodney Nelsestuen, June 20, 2011, in his publication 'Why Breaches Happen and What to Do About it' asked the question why there is an increase threat to data security in the banking institutions. As this continue to be a major concerns firms should ensure that outsourcing vendors follow best practices in human resources such as performing suitable background checks and screening employees, Boston Globe, August 2011. Additionally, entering into a non-disclosure agreement with the outsourcing vendor also goes a long way in maintaining high privacy standards.

Banking and financial institutions have failed to address the problems of data protections due to poor information management systems within the structures of its administration, Treacy, W. F., & Carey, M. (2000). The cost implications of a data breach from both monetary and reputational perspective are increasing exponentially for financial firms. Accordingly, to Davenport, T. H. (2014). The risk management team of every financial service institute needs to play an active role in shaping policies regarding data security, information management and the use of advance systems and applications in close partnership with their technical team.

In terms of the knowledge gap in in the use of advance technology, poor access to internet facility, storage system and electricity shortage are the major factors that are considered to be overwhelming challenges affecting banks and financial institutions in under developed countries, European Central Bank. (2014). Lot of information and communication technology comes with great challenges that has to do with system failure as a result of the highlighted problems in the above statement.

2.1.2 Literature Relating to Different Variables

The followings can be referred to as the different process or activities that has to do with data protection and management. Every organisation has a data management system that is both hardware system and software: **Data privacy:** Data privacy refers to appropriate use of data provided to corporations for agreed purposes. Data collected by customers to meet the business requirements and need of customer should be sufficient; it should be accepted by customer and with complete disclosure information being provided to them. Ohm, Paul. 2010. Australian Federal Government continues to impose penalty for not providing enough disclosure to customers about data privacy. In banking and financial services industry, the data collected is to ensure identity of customer and it is called as Personally Identifiable Information. **Data security:** Data security refers to confidentiality, availability and integrity of data. The data security means it is accessible, used and processed by authorised users only. Data security ensures it is available, reliable and accurate, Edwards, John. 2010. Data security plan ensures collecting only required information, keeping it safe and destroying any

information which is no longer needed, Michael H. Keller, and Aaron Krolik. 2018. **Information privacy:** Information privacy refers to the desire of individuals to control or have some influence over data about themselves. Information age has lead us to four major concerns about the use of information: privacy, accuracy, property and accessibility. Clarke (1999), identified four dimensions of privacy of person, personal behaviour, personal communication and personal data privacy. Today most communication channels are in digital form through mobile phones and internet, so the personal communication privacy and personal data privacy are merged into information privacy. **System security:** Systems security refers to its ability to protect from external attacks (Deliberate or accidental). Secured systems make them dependable and available when required, thus makes them reliable.

2.1.3 Literature Relating to Specific Combination of Variables

Data protection is defined as "the process of safeguarding important data from corruption, compromise, or loss; and providing the capability to restore data to a functional state should something happens to render the data inaccessible or unusable.

There are three broad categories of data protection: traditional data protection, data security, and data privacy. Traditional data protection has to do with the physical infrastructure of data protection during the entire data management lifecycle, from data storage and backups to archiving and deletion. On its own, traditional data protection has some noteworthy limitations. For example, it's usually confined to the data centre perimeter, Qian Tang et al. 2013.

Ultimately, each type of data protection is important and aims to prevent some of the data protection challenges. A robust data protection strategy should include each of these data protection categories to assure that it's covered from all angles.

Physical security threats: Although it might be one of the least glamorous and most neglected aspects of data protection, physical security is critical for thorough data protection strategy. After the onset of the COVID-19 pandemic, many physical workspaces (offices, campuses, and even data centers) were suddenly and almost entirely unoccupied. The devices, data, and other organizational assets that were left behind became even more vulnerable to theft, alteration, or even deletion, Kevin Kelly, (2009).

Insiders' threats: A constant concern in the business community is the risk of insider threats. While most organizations don't want to admit that their employees might be capable of executing internal attacks on their systems and networks, the area unfortunately warrants further exploration. Holding your employees accountable, especially in the midst of the remote work revolution, can be a difficult task. There are, however, some steps you can take to prevent insider threats from becoming security incidents. We will explore those later when we introduce some of the best practices for overcoming data protection challenges.

Cyber ecurity threats: Even as the digital transformation continues to revolutionize how organizations use technology, the weakest link in the cyber security chain will probably always come down to human error. In particular, social engineering attacks such as phishing emails remain one of the most common ways in which malicious actors gain unauthorized access to systems and networks. Phishing emails sometimes even contain ransom ware, a growing threat in the business community. Employees who unknowingly click on a malicious link or download malicious software (malware) can put your entire organization and its customer data at risk.

Corporate Culture: The first (and probably least obvious) data protection challenge is an underlying corporate culture that doesn't take cyber security seriously. Most organizations, and especially small to medium businesses, are shocked when they experience a security incident because they simply never imagined that they could be the victim of a cyber-attack. Many small medium businesses truly believe that their data isn't valuable to cybercriminals; they are wrong. Most of the time, cybercriminals target smaller businesses precisely because they know those businesses are less likely to have a robust cyber security program in place, which makes them an easier target.

Regulations: As data protection gains more traction in the business community and among consumers, it's likely that the number of regulatory requirements affecting businesses that deal in personal data will continue to grow. One of the most well-recognized and widely enforced regulations is the General Data Protection Regulation, which applies to any organizations collecting data from people residing in the European Union.

2.1.4 Data Protection and Financial Regulations

Many firms are failing to identify all aspects of the data security risk they face, for three main reasons. First, Data some do not appreciate the gravity of this risk; second, some do not have the expertise to make a reasonable assessment of key risk factors and devise ways of mitigating them; and third, many fail to devote or coordinate adequate resources to address this risk, Parsheera, Smriti. (2011). Large and medium-sized firms generally devote adequate resources to data security risk management but there is a lack of coordination among

relevant business areas such as information technology, information security, human resources, financial crime, and physical security, Loucks, Jeff. 2018.

There is too much focus on IT controls and too little on office procedures, monitoring and due diligence. This scattered approach, further weakened when firms do not allocate ultimate accountability for data security to a single senior manager, results in significant weaknesses in otherwise well-controlled firms, Matthan Rahul 2017. Firms' risk assessment of their exposure to data loss incidents is often weak. Some make no risk assessment at all and only a few continuously monitor the effectiveness of their data security controls. In some medium-sized and small firms, there is a lack of awareness that customer data is a valuable commodity for criminals. As a consequence, systems and controls are often weak and sometimes absent, Cakebread, Caroline. 2012.

Now, with several well-publicised incidents of data loss during 2007, nobody in the UK can claim ignorance of the risk of customer data falling into the wrong hands. It is good practice for firms to conduct a risk assessment of their data security environment and implement adequate mitigating controls, Dobkin, Ariel. 2018. If firms consider that their in-house resources or expertise are inadequate to perform a coherent risk assessment, they should consider seeking external guidance, Pichai, Sundar (2019). Our experience of dealing with data loss incidents shows that firms often fail to consider the wider risks of identity fraud arising from significant cases of data loss.

Many firms appear more concerned about adverse media coverage than in being open and transparent with their customers about the risks they face and how they can protect themselves, Balkin, Jack M. 2016. However, some firms which suffer data loss are beginning to take a more responsible approach by writing to their customers to explain the circumstances, give advice and, in some cases, pay for precautions such as credit checking and Protective Registration. In most firms, more-stringent vetting is applied to staff in senior positions. There is little consideration of the risk that junior staff with access to large volumes of customer data may facilitate financial crime. Consequently. Loucks Jeff, 2018, argues that very few firms conduct criminal record checks on junior staff. In addition, few firms repeat vetting to identify changes in an individual's circumstances which might make them more susceptible to financial crime. Data security policies in medium-sized and larger firms are generally adequate but implementation is often patchy, with staff awareness of data security risk a key concern. Trainings for front-line staff (e.g. in call centres), who often have access to large volumes of customer data, is rarely relevant to their day-to-day duties and focuses more on legislation and regulation than the risk of financial crime, Warzel, Charlie. 2019.

This means staff are often unaware of how to comply with policies and do not know that data security procedures are an important tool for reducing financial crime. In addition, many firms do not test that their staff understand their policies. Access to customer data via computer systems and databases is generally well controlled in large and medium-sized firms, with a general aim of only allowing staff to access information that they specifically require to do their job. In small firms, it is not unusual for all staff to have access to all customer data.

Firms' dealings with third-party suppliers are a major concern. Many firms, small and large, use third parties for IT maintenance, as well as the backing up of electronic files and archiving of paper documents. Firms generally rely too much on assumptions that contractual terms are being met, with very few firms proactively checking how third parties vet their employees or the security arrangements in place to protect customer data. In addition, some firms do not consider the risk associated with granting third-party suppliers such as cleaners and security staff access to their premises, McLean, Rob. 2019.

Large and medium-sized firms tend to transfer data to and from third parties using secure internet links but there are still occasions where data is transferred on compact disc or mainframe cartridges. We observed that these items are not always encrypted. On rare occasions, firms are sending unencrypted customer data by unregistered post. Large and medium-sized firms usually recognise the risks of data loss via laptops, USB devices and the internet.

2.1.5 Policies and Procedures

If a firm's management is committed to ensuring data security, it is likely to have specific written policies and procedures covering the subject. However, Sathe Gopal. (2019), in his first publication on data management was not convinced by firms that claimed to have detailed data security rules but were unable to produce written policies and procedures. Indeed, the existence or absence of an up-to-date, accurate and relevant data security policy can be a telling indication of whether the firm really understands the risk and takes it seriously.

Firms with large or complex operations tended to have detailed policies and procedures. Typically, the data security policy was a high-level document supplemented by more detailed procedures and guidance for different business areas relating to the specific risks they faced, Madrigal, Alexis C. 2012. Small firms, with their more-manageable risks, did not always have formal policy documents and used simple guides of 'Do's and Don'ts' as

an effective way of setting out expectations and communicating them. However, in a worrying number of cases, firms failed to record policies and procedures at all.

In these firms, senior management were effectively relying on the judgement of individual staff often with little or no understanding of the risks as their only data security control. This approach was typical of some small firms whose managers appeared to treat data security more as a matter of office administration than as a potentially significant risk that could affect their business, reputation and customers.

Good policies and procedures specify exactly what staff and contractors must do and not do to comply with expected standards and provide the means for enforcing them. Firms that do not set out or communicate clearly the standards they expect are running the risk that their staff do not understand what is expected of them; data security risk in these firms is likely to be high.

2.1.6 The Benefits of Information Management System

According to Cham Switzerland. 2017, Information management systems are used in many industries and sectors. They are used to store, process, and share different types of information with other people or entities. With an information management system, we can make sure that the data is secure and available at all times. Information management systems are a necessary part of any business. They can be used to improve business processes, increase productivity and reduce costs. These benefits can be referred to as: **Increase productivity:** An Information management system is an integral part of any business, organization or company. An Information management system helps to organize and store all important information in one central location. This enables employees to be more efficient, productive, and ultimately successful. **Improved communication:** It is important to have an IMS that can capture and control the flow of data in a company. It will help improve communication with customers, employees, partners and suppliers. With an effective system in place, teams can ensure there are no miscommunications or missing information which would reduce customer satisfaction. It will also help you find the data you need as quickly as possible. **Reduce errors:** There are many benefits to implementing an effective information management system. It helps reduce errors by helping employees find the right document or file for their needs. It also helps with the many hours of paperwork that are necessary at an agency. **Increase competitive advantage:** In the digital age, the way companies manage and store data has a big impact on their success. A report from Forrester Research shows that in an era of growing customer demands and accelerating competitive pressures, every organization needs an information management strategy to be "data-driven. **Cost savings:** There are many benefits to implementing an effective information management system. One benefit is cost savings. Information is expensive to store and maintain, but with the right system, that expense can be greatly reduced.

2.1.7 Information Security Management in Banking and Financial Services

Banking and financial services considers below measures for information security and privacy while using cloud computing architecture infrastructure through **Identity Access Management (IDM):** This mechanism helps to authenticate users and services based on credentials and characteristics. Bélanger, F., and R. E. (2010). Credentials means "User Identity" (or Unique Network ID and Password) and Characteristics means defined method of running cloud services. In banking and financial services industry, when the personally identifiable information of customer and their financial history is available over cloud architecture, it is very important to identify users who are accessing information. An identity access management system helps to protect access levels of users by identifying them based on roles and responsibilities.

Access Control and Access Logging Mechanism: Cloud services delivery models have complex architecture. This complex architecture needs to be integrated with access control interfaces that demands policy neutral access specification and enforcement framework. In order to control access, Single Sign-On (SSO) method is implemented which gives access to user across multiple applications in banking and financial services, Müller-Bloch, C., and J. Kranz 2005. These access methods confirm one time identification of user based on "Single User Id / Network Id" and password that meets security policy, McConnell, and H. J. Smith 2001. Access logging or User Activity monitoring is collecting and storing the logs of users who are using, operating and maintaining cloud infrastructure. User activity monitoring helps to keep record of the all the changes performed on data and applications over cloud infrastructure.

Roles Based Access Control and Malicious Insider: Cloud computing is shared infrastructure for employees, customers and third-party service providers. Role Based Access control governs the access to information and ensure that users have right level of access as per roles and responsibilities. Role based Access control is importance to avoid exposure of data to user that are not supposed to use it in any form. Malicious insiders is user with access to system at the same time lack of identity, authentication and having control over use of system. With privilege accesses, users can view and use information that may be termed as data theft. In order to maintain confidentiality of business information, access control and control over malicious insider is considered.

Governance and Compliance: Cloud security governance consists of leadership, organization structure and processes that safeguard information. Compliance is requirements from government regulatory bodies to adhere to rules in order to function within framework. Governance and compliance ensure the strategic alignment of system with customer, business and employee needs. Governance and Compliance department in banking and financial services industry help to provide over all working, monitoring, measuring and communication framework to keep cloud architecture secure, Greenaway, K. E., Y. E. Chan (2022).

Service Level Agreements (SLAs) and Contracts with Cloud Service Provider (CSP): Cloud computing infrastructure is availability of computing resources from any remote location at any time. In order to meet these requirements, cloud services should be monitored and maintained well. Cloud service providers are located across geographies, so the contracts is between legal jurisdictions of two nations. De Hert, P., and V. Papakonstantinou (2000).

These contracts must be in accordance with needs to cloud infrastructure user. These contracts must acknowledge data privacy and data security related aspects to protect sensitive details of various customers. So, SLAs and contractual agreements are considered as important for smooth running of cloud services, which in turn help smooth running of banking operations.

Despite, the studies reviewed provide valuable knowledge and understanding from different perspectives about the composition, role, limitations, importance and impact of data protection and information management in financial institutions.

2.2 Research Methodology

This survey was conducted over a 2-week period with two indigenous and two foreign banks in Sierra Leone in June/July 2024. A questionnaire was developed, which comprised two segments; first segment focused on individual interview while the other segment focused on group interview. The questions were open and close-ended. The questionnaire was divided into two parts and five sections - A, B, C, D and E. Part I, Section A had questions bothering on personal details of the respondents; while Part II, sections B, C, D and E were based on each objective. The researchers adopted the drop and pick method whereby the respondents from selected departments were required to complete the questionnaire at their convenience because of the busy scheduled while the group discussions were done with minimum of 5 respondents in order to obtained quality responses. A total of 60 questionnaires were distributed, however, 50 respondents completed the questionnaires; the survey had a response rate of 83%.

II. FINDINGS AND DISCUSSIONS

3.1 Demographic Characteristics

Data were obtained from 50 respondents from selected departments within the R Bank. The demographic factors revealed that there were more female (57%) and male (43%). This indicates that there are more female respondents for this study. The analysis revealed that 28% of respondents were between 18 – 35 years, 52% were between 36 - 50 years, these 2 categories are individuals with have good understanding and are readily willing to provide useful information on the subject matter of the research while 20% of the respondents fall under 50 years and above category. The educational level of respondents who participated in the study, 20% had attained graduate (Masters) degrees, 50% had first (BSc.) degrees while 30% had only diplomas.

RQ1: Causes of Poor Data Management and Security in Financial Institutions

According to the analysis, the findings reveal that storage space, human errors, network problems, and a number of inexperienced personnels deal with data management in the R Commercial Banks. These causes are obvious because R Bank has over the years experienced a rapid increase in the number of customers and partners as a result of introduction of modern technology in the banking systems. However, these also led to the expansion of their markets across the country with the establishment of sub-branches across the nation. Most importantly, the banks have gained more competitive edge in online banking as a strategy. Therefore, these gains come with numerous challenges in data management that are affecting the effective and efficient operations of these banks.

Secondly, human errors and network problems are another set of key factors that cause poor data management in the R Commercial Bank. The respondents revealed that poor data management in the bank is a serious challenge to the banks and their customers and this has affected customers' relationship with some branches especially in the provincial regions. However, most of the respondents do believe that their bank has adequate and experienced personnel charged with the responsibility to ensure effective data management and security of their operations. The revelation indicates that the performance and contribution of the staff in the institution could be considered to be satisfactory to the management and its customers despite the challenges.

RQ2: The Significance of Data Protection and Information Management

With reference to the analysis revealed that data protection and information management is very significant to the operations and success of the R Commercial Bank. However, according to the analysis, it reveals that 40% of the respondents say that data protection and information management system is effective but needs more improvement in the bank as the bank need to train more staff in the subject area, while 60% of the respondents indicated that information management in the banks is very effective and this has helped the bank gain competitive edge in the banking industry in Sierra Leone.

Also revealed in the analysis, that data protection has been a challenge for R Commercial Bank to address because of unreliable internet connectivity and frequent system downturn, working environment, unreliable electricity supply, human errors, and poor network system. However, the study reveals that these are the fundamental factors that limit these commercial banks in gaining competitive edge in the banking sector in Sierra Leone. In response to these challenges faced with data protection and information management in these banks, the Researcher, therefore, asked questions in line with the objective of the research to proffer the best options on how to address the problem highlighted in the above statement. In line with the aforementioned, according to the respondents, 40% of the respondents indicated that in solving the problem of data security and information management, there should be uninterrupted electricity supply while 60% of the respondents say that a strong internet facility can address the problem.

RQ3: Impact of Data Protection and Information Management

Data protection and information management in the banking sector is a very strategic function that can easily undermine the reputation of the commercial banks. The banking policies in line with data protection and information management must ensure customers' confidentiality, privacy of information, and protection of sensitive information from third parties. However, based on previous experiences and challenges in relation to data protection, commercial banks have in recent times with the aid of integrated technological systems, the have developed systems and applications that ensure data security, information management, and innovation to address its challenges.

According to the study it has helped to improve the banking business, and it has opened more doors of opportunities to customers and employers to explore new ideas. Therefore, it is also important to note that information management has changed the way the commercial banks operate with the deployment of more advanced systems. Information management and data protection have helped to build customers' confidence and strong working relationship with commercial banks and their partners across the country. Also, with the rapid development and the growing challenges in the banking sector, these have led to implementation systems in order to reduce the risk in data security and information management in the banks. In the past decades, there have been cases of internet fraud, information leakages, human errors, poor networking systems and internet connection, amongst others, which confirms some of the findings relating to challenges from previous researches.

RQ4 The Importance of Data Protection in Financial Institutions in Sierra Leone

The findings revealed that data protection is very important to the successful operations of all financial institutions and not only at the R Commercial Bank. Data protection is not only considered as being significant to the operations of financial institutions but it also protects them from collateral damage and lack of trust and confidence by their customers. According to the respondents, 48% believe data protection is very important for successful operations, 20% believe it is important, another 20% believe it is somewhat important, on the contrary, only 8% believe data protection is not important while 4% indicated they had no idea.

4.0 CONCLUSIONS AND RECOMMENDATIONS

4.1 Conclusion

The primary objective of this research was to assess data protection and information management in Financial Institutions and the R Commercial Bank as a case study. From the findings, it is evident that this is a very serious challenge that undermines the effectiveness and efficiency of banking operations. However, the objective of the findings is to understand the significance of data protection and information management, and how it affects and contributes to the operations of the Bank and other financial institutions.

The findings in the analysis reveal that data protection and information management in the R Commercial Bank have encountered numerous problems that have posed a threat to data security and information management. According to the study data and information management have led to the transformation of mot only the R Commercial Bank but other financial and banking institutions in order to achieve their primary objectives. Therefore, the analysis of the findings identifies the gaps in data protection and information management in the R Commercial Bank. It points out that there is a lack of effective policy

formulation and implementation to address that insecurity and information in the bank. Most of the problems encountered in the operations of the Bank are related to poor information management and data insecurity.
Finally, the analysis of data collected in the research clearly defines the objectives of the research, outlines key findings, extensively analyses the problems, and provides possible options that can address the problems highlighted.

4.2 Recommendations

There is the need to improve the systems deployed for data protection and information management as well as embark on frequency capacity building of the personnel charged to handle such sensitive information of all financial institutions in Sierra Leone. In terms of what needs to be done to address the problem of information management and data security in the commercial banks; the following recommendations are put forth as measures in order to tackle the problems and/or challenges:

- **Minimisation of Data** – data minimization is considered a core principle of data privacy regulations, which will require any organisation especially the bank sector to only harvest strictly necessary data;
- **Encryption of data** – Banks must adopt a policy of encrypting data before the are transmitted to as to avoid being intercepted by cybercriminal;
- **Automated Monitoring -** continuous monitoring of data access and usage helps detect when there are anomalies or system breaches;
- **Uninterrupted electricity supply:** This will be a fundamental solution to address the problem of frequent shortage of electricity supply that affects and delays the effective functioning of the commercial banks. According to the respondents, the interruption of electricity supply during the day affects online transactions and other operations that have to do with the internet. The findings indicate uninterrupted electricity supply will save time, prevent loss of data, and ensure efficiency in service delivery in the banks;
- **Training of more ICT Staff:** Frequent capacity building of the concerned staff will help to address some of the numerous challenges that the commercial banks are encountering. The findings indicate that there is a need for the commercial banks to train competent and qualified ICT staff with the requisite skills and experience to ensure data protection and information management are accurately administered in all departments of the banks;
- **Installation of a good network system and strong internet connectivity**: according to the respondents, this is very significant to a successful customer service delivery as the findings revealed that poor internet and networking system has been one of the factors that undermine quality service delivery in the commercial banks; and
- **Financial Policies:** Implementation to the letter of all financial policies as stipulated by the Central Bank, which is the Bank of Sierra Leone.

REFERENCES

[1]. Bélanger, F., and R. E. (2010). Improving security of interest banking system using three –level security implementation,

[2]. Biswal, S. P., & Kulkarni, M. S. (2021). Implications of GDPR on emerging technologies. Revista Gestão Inovação E Tecnologias, 11(4), 4898–4912. https://doi.org/10.47059/revistageintec.v11i4.2512

[3]. Chan, K. E., Y. E. (2022), Information processing as an integrating concept in organizational design. Academy of Management Review, 3, 613–624.

[4]. Firms enlist smartphones to provide cyber security, Boston Globe, August 2011

[5]. Jun, M., & Cai, S. (2001). The Key Determinants of Internet Banking Service Quality: A content analysis. International Journal of Bank Marketing, 19, 276–291

[6]. Loucks Jeff, 2018, Data to knowledge: Building an analytic capability. California Management Review, 43, 117–138

[7]. Outsourcers look to data security transparency for competitive advantage, www.computerweekly.com, July 2011.

[8]. Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Research in International Business and Finance, 60, 101616. https://doi.org/10.1016/j.ribaf.2022.101616

[9]. Seese, D., Weinhardet, C., & Schlottman, F. (2008). Handbook on information technology. Finance. New York: Springer.

[10]. Serrado, J., Pereira, R. F., Da Silva, M. M., & Bianchi, I. S. (2020). Information security frameworks for assisting GDPR compliance in banking industry. Digital Policy Regulation and Governance, 22(3), 227–244. https://doi.org/10.1108/dprg-02-2020-0019

[11]. Tilson, D., Lytinen, K., & Sørensen, C. (2010). Digital infrastructures: The missing IS research agenda. Information Systems Research, 21, 748–759

[12]. Treacy, W. F., & Carey, M. (2000). Data Intensive Applications, challenges, techniques and technologies: A survey on Big Data.

[13]. Uzougbo, N. N. S., Ikegwu, N. C. G., & Adewusi, N. a. O. (2024). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. International Journal of Science and Research Archive, 12(1), 533–548. https://doi.org/10.30574/ijsra.2024.12.1.0802

[14]. Voglhofer, T., & Rinderle-Ma, S. (2019). Collection and Elicitation of Business Process Compliance Patterns with Focus on Data Aspects. Business & Information Systems Engineering, 62(4), 361–377. https://doi.org/10.1007/s12599-019-00594-3

Oludolapo O. Akinyosoye–Gbonda (Ph.D.)
Institute of Public Administration and Management – University of Sierra Leone