

# **Impact of Audit Trails on the Financial Audit of Nigerian Banking Sector**

**BANA, Joseph O.**

Department of Accounting  
Bingham University  
Karu, Nasarawa State

E – Mail: bana\_joe@yahoo.com, Phone No: +234 8059311652

## **Abstract**

*Every human endeavour attracts foot-prints in the sands of time. These foot-prints can be positive or negative, beneficial or detrimental in the nearest future. This is synonymous with the workings of audit trails. This study examines the impact of Audit Trails on the Financial Audit of Banking Sector. A causal research design was adopted with reliance on primary and secondary data obtained from published and unpublished literatures to explain the relationships between the variables. A simple random sampling technique was used in the selection of Audit Firms of twenty (23) Commercial Banks in Nigeria to confirm the veracity of the subject. Data collected were analyzed by descriptive statistics and presented through frequency distributions and percentages using the Likert scale. The chi-square contingency procedure was used to test the hypothesis. The findings revealed that Audit Trails have significant positive impact on the financial audit of the banking sector. It further reveals that Audit Trails of the Financial Audit of Banking Sector has impact on fraud detection; disaster recovery; assist in the recovery of lost transactions and have impact on regulatory compliance. The study affirms that Audit Trails are not only used as tools in determining the validity of an accounting entry, source of funds or trade, but protect businesses from liability during legal battles, help monitor data for security breaches, ensures that proper protocols are followed and demonstrate compliance.*

Keywords: Audit Trials, Financial Transactions. BankingSector, Financial Audit.

## **INTRODUCTION**

Every audit is carried out on the basis of managing the ‘‘who, what, and when of business transactions’’. Having an accounting audit trail for every transaction combats errors in financial reporting by reducing the risks that come with both missing or incomplete data and fraud. Full transparency makes it easy for auditors or examiners to confirm that information is accurate and complete, and aid the team in identifying areas for potential process improvement. An audit trail is a step-by-step record by which accounting or trade data can be traced to its source. It provides basic information to backtrack through the entire trail of events to its origin, usually the original creation of the record. This may include user activities, access to data, login attempts, administrator activities, or automated system activities. Audit trails are used to verify and track many types of transactions including accounting or banking transactions. An audit trail is most often utilized when the accuracy of an item needs to be verified. Audit trails can be useful tools when determining the validity of an accounting entry, source of funds or trade. At its most basic level, every business needs an audit trail of its financial transactions, which includes accounts receivable, accounts payable, invoices and purchase orders. In other words, audit trails comprise what was once referred to as the ‘‘paper trail’’ of business. Having a detailed audit trail can protect a business from liability during legal battles, help monitor data for security breaches, ensures that proper protocols are followed and demonstrate compliance.

## **LITERATURE REVIEW**

### **Conceptual Framework**

#### **Auditing, Types and Objectives**

Auditing refers to the periodic examination of accounts, documents, and vouchers in a corporate world. It is nothing but an inspection of all the financial and statutory records relating to the company’s financial position. Auditing takes place in both the corporate and public sectors and it recognizes all the possible pieces of evidence that evaluates and formulates the opinion base on communication they carry out. It is

nothing but an analysis of the current system, reports, and process of the organization. Types of auditing include but not limited to: Construction audit, Tax audit, Investigative audit, Financial audit, Information system audit/Information Technology (IT) Audit, Compliance audit and Operational audit

The main objective of the auditing is to provide a suggestion on financial reports and statements. For this, the auditor needs to analyze all the financial statements to check the financial position of the entity. Auditing does not cover all the errors and frauds that happened with the help of financial reports provided. Objective of auditing includes: Analyzing the internal system; Checking the authenticity and validity of transactions; Examining arithmetical accuracy of books of accounts, casting, balancing; Finalizing the current value of assets and liabilities and Inspecting the variance between capital and revenue type of transactions. It also includes: Finding and preventing errors; Finding and preventing of frauds and Unusual stock valuation.

### **Audit Trails**

An audit trail is a step-by-step record by which accounting or trade data can be traced to its source. Audit Trail is defined as a chronological sequence of records that contain evidence about a business process. An audit trail (also called audit log) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. Audit trails are the manual or electronic records that chronologically catalog events or procedures to provide support documentation and history that is used to authenticate security and operational actions, or mitigate challenges. Audit trail records will contain details that include date, time, and user information associated with the transaction.

### **Financial Audit**

All public companies undergo a financial audit as part of their reporting responsibilities. Financial audits conducted to provide an opinion whether financial statements (the information being verified) are stated in accordance with specified criteria. In providing an opinion whether financial statements are fairly stated in accordance with accounting standards, the auditor gathers evidence to determine whether the statements contain material errors or other misstatements. Financial audit's purpose is to evaluate whether an organization is adhering to standard accounting practices. Information Technology (IT) plays an important role in the general process of the financial audit of banking sector, industry- or regulation-specific audit logs and trails. An audit trail provides a tool to maintain information and system integrity.

### **Banking Sector**

The banking sector is an industry and a section of the economy devoted to the holding of financial assets for others and investing those financial assets as a leveraged way to create more wealth. The sector also includes the regulation of banking activities by government agencies, insurance, mortgages, investor services, and credit cards.

### **Different Schools of Thoughts about Audit Trails**

Organizations support compliance, security and operations. Different laws make audit records important element in defending against security breaches, supporting compliance reporting, and ultimately passing numerous kinds of internal and external audits. There are many definitions of an audit trail, and all of them give an idea of what it is about. An audit trail consists of records that document every step in a business transaction. This may include initiating documents, processes, authorization and approvals. It also means invoices for payments issued or sales contracts documenting revenue. Payroll and other human resource records prove correct treatment of employees. Start-ups and businesses must pay close attention to maintaining such records. A complete audit trail proves to investors or lenders and users the validity of information on the financial statements, and meets government record keeping requirements for tax purposes. It is a system that traces the detailed transactions relating to any item in an accounting record. It is a record of the changes that have been made to a database or file. Each record in audit trail

includes information about who created the record, with what system, on what date and at what time. A data log captures the records that make up an audit trail, and audit trail reports assemble these records so that analysts can scrutinize them. Audit trail reports serve business purposes such as lost transaction recovery, fraud detection, disaster recovery and regulatory compliance.

It is a general principle that well-managed audit trails are key indicators of good internal business controls. Audit trails have transitioned from manual to automated electronic logs that make historical information more accurate, readily accessible, and usable. Successful audit trails demand a top down commitment by upper management, affected departments, and information technology (IT) personnel. The more quickly an abnormal change or addition to information is “red-flagged,” the better the response to mitigate against negative influences such as cyber-threats, security breaches, data corruption, or misuse of information. Audit trails, or rather the process of following an audit trail, are found in many different areas of finance. With any financial accounting system, it’s imperative to be able to understand and control changes within a company’s financial system. This is critical not only from a regulatory perspective, but also for risk management and fraud prevention. Numerous industries use versions of an audit trail to provide a historical record of progression based on a sequence of events. These records provide proof of compliance and operational integrity. Audit trails can also identify areas of non-compliance by providing information for audit investigations. Whether it is logging the design changes of a product build, keeping the record of financial transactions for an e-commerce site, communication transactions, healthcare activity, and financial audit of banking sector or legitimizing the outcome of an election, an audit trail validates actions and outcomes.

### **Tools for analyzing Audit Trails**

The multiple number of events included in an audit trail calls for automating the collection of audit trail information. Tools that have trend analysis and detections for unusual use can lead to breaches. Red-flag warnings for unauthorized log-ins (whether successful or not) provide attack detection. Functions that follow defined user activities can identify misuse to prevent the theft or corruption of valuable data. Identifying application or system failures is also a key aspect for continuous operations and to prevent unscheduled outages or downtime. Audit trail reviews vary by organization and may take place quarterly or annually during a security audit. Audit trails provide the means to backtrack a vast array of problems associated with information security, access, and system optimization. The balance between system protection and operational performance should be maintained at industry appropriate levels.

### **Empirical Literature**

An audit trail provides basic information to backtrack through the entire trail of events to its origin, usually the original creation of the record. This may include user activities, access to data, login attempts, administrator activities, or automated system activities. Audit records contain element defined by the company. Some audit trails look more closely at actions within certain applications to chronicle more than a simple system or application launch. These logs can pinpoint elements such as specific changes to a database or information contained therein, and can also detect improper web-browsing or email use. Audit trails maintain a record of system activity. They leave a series of records of computer events about an operating system, applications and even user activities. This ensures that system resources have not been harmed by hackers, insiders, disgruntled employees, and technical problems that may arise. An audit trail is made up of business's financial transactions and it is important because it helps prevent fraud. Many information technology (IT) departments have more than one audit trail that can be system-application or event-defined. Highlighting abnormal activities or use deemed "out of the ordinary" can initiate an investigation. An accurate and well-defined audit trail provides the evidence to find answers and solve issues.

Information Technology (IT) Audit Trails are constructed to address numerous activities that make up an event or series of events that can be investigated to find areas of concern. Problem activities include security breaches from hackers, in-house or out-of-house authentication problems, unauthorized usage, unusual levels of activity, or system failures. Records include the automated events scheduled through the operating system (OS), network access, application events, and manual activities of the various users.

The need to support compliance, security, and operations is found in most (if not all) industries. The laws that both mandate and regulate the use of electronic records make audit records an important element in defending against security breaches, supporting compliance reporting, and ultimately passing numerous kinds of internal and external audits. Industries that have provisions to track information integrity include government agencies who maintain sensitive, confidential information, and any company that uses electronic records containing confidential information such as the Banking Sector. Audit trails are commonly managed by Auditors and backend staff within the information technology (IT) department, such as a security manager or network administrator. A key point to keep in mind is that any user, whether a manager, employee, end-user, legal staff, an accountant, or others who touch an electronic record, will be included in the audit trail of the record. This user may be a human who makes an update to a record or accesses a system, or it may be a system that automatically makes update/changes such as restarting a computer.

### **Theoretical Discussion**

The ability to follow records back to their origin provides numerous benefits, including transparency and a defense of records for compliance, record integrity and accuracy, system protection from misuse or harm, and security of sensitive or vital information. These are achieved through the four critical areas namely Users, reconstruction of events, Intrusion Detection and other problem identification. A user is anyone who has access to the system. Implementing audit trails promotes appropriate user behavior, which can prevent the introduction of viruses, improper use of information, and unauthorized use or modifications. In addition, the user knows that their actions are automatically recorded and tied to their unique identity. When an investigation is warranted or triggered, the first step to remediate a problem is knowing the "when," the "how," and the "what" of the event. Visibility into this information can aid in problem detection and prevent future occurrences of things such as hacking, system failures, outages or corruption of information. Audit trails aid in identifying suspicious behavior or actions. Unauthorized access is a serious problem for most systems. Many regulations now have mandates for the security of information and maintaining confidentiality. Protection also extends to intellectual property, designs, personnel information and financial records. Through real-time monitoring, you can use automated audit logs to identify problems that indicate system implementation issues, operational issues, unusual or suspicious activities, or system and operation errors. The audit trail provides a "baseline" for analysis or an audit when initiating an investigation. The purpose or importance of an audit trail takes many forms depending on the organization: A company may use the audit trail for reconciliation, historical reports, future budget planning, tax, or other audit compliance, crime investigation, and/or risk management.

### **METHODOLOGY**

In carrying out this study, both primary and secondary data was employed. The secondary data is derived from library documents, publications and Internet, and other relevant materials. The primary data are obtained through questionnaires and interviews. The study incorporates both sources of data to enhance a balance between the research observations and available literature on the matter under consideration. Interview was adopted in order to increase the depth of the study as well as obtain sensitive and salient information about the issue under review, which could not be obtained through questionnaire. In short, the interview provided an opportunity for meeting with some of the respondents (External Auditors and the Bank Officials) and discussions helped the researcher to obtain other pertinent information, which greatly assisted in the findings herein. The choice of the description survey research design was made

*Impact of Audit Trails on the Financial Audit of Nigerian Banking Sector*

based on the fact that in the study, the researcher was interested on the state of affairs already existing in the field and no variable was to be manipulated. The study population was twenty-three (23) Commercial Banks in Nigeria and their corresponding seven (7) External/Independent Auditors.

Qualitative data collected was analyzed by descriptive statistics and presented through frequency distributions and percentages using the likert scale on a scale of 5-1. The chi-square contingency procedure was used to test the hypothesis. The variables are extracted from the questionnaires and the stipulated level of significance value of five (5) per cent (0.05) was selected. The decision is that if  $X^2_{cal} > X^2_{tab}$ , reject  $H_0$  and Accept  $H_1$ . The sample size of 60 respondents was taken from the twenty three (23) Commercial Banks and their seven (7) Independent Auditors in Nigeria. The sample size was calculated using 95% confidence interval.

$$n = \frac{N}{1 + N(e)^2}$$

Where:

N=Population

n=Sample size

$$e = \frac{(0.05)^2}{60}$$

$$n = \frac{60}{1 + [60(0.0025)]} \quad \text{Sample size =60}$$

The data collected in this study was analyzed statistically by the use of frequency tables and percentage and Chi Square method.

$$X^2 = \sum \frac{(o - e)^2}{e}$$

Where  $X^2$  = Chi - Square

**F<sub>o</sub>** = Frequency Observed

**F<sub>e</sub>** = Frequency Expected.

The hypothesis formulated is tested by means of the  $X^2$  – Chi - Square. As a decision rule, if the computed value of  $X^2$  (Chi–Square) is greater than the critical value of  $X^2$  (Chi–Square) at 5% level of significance, the null hypothesis (**H<sub>0</sub>**) is rejected, while the alternative hypothesis (**H<sub>1</sub>**) is accepted. The reverse is however the case if the computed value of  $X^2$  (Chi-Square) is greater than the critical value at the chosen level of significance. Analysis of the questionnaires and interviews in line with the impact of Audit Trails on the Financial Audit of Banking Sector reveal the following responses

Likert scale	Frequency	Percentage	Valid Percent	Cumulative Percent
STRONGLY AGREE	37	61.6	61.6	61.6
AGREE	10	16.7	16.7	78.3
DISAGREE	9	15.0	15.0	93.3
STRONGLY DISAGREE	4	6.7	6.7	100.0
<b>TOTAL</b>		<b>100.0</b>	<b>100.0</b>	

**RESULT AND DISCUSSION**

**Test of Hypothesis 1 - Question 1 and 2**

**H01:** Audit Trails of the Financial Audit of Banking Sector has no fraud detection.

**Table 2**

RESPONSES	STRONGY AGREED	AGREED	STRONGLY DISAGREED	DISAGREED	TOTAL
QI	22	17	10	11	60
QII	38	11	8	3	60
<b>TOTAL</b>	60	28	18	14	120

$$X^2 = \frac{\sum (o - e)^2}{e}$$

**Table 3**

O	E	O-E	(O-E)2	(O-E)2/E
22	30	-8	16	0.533
17	14	3	9	0.6429
10	9	1	1	0.111
11	7	4	16	2.286
38	30	8	64	2.133
11	14	-3	9	0.6429
8	9	-1	1	0.111
3	7	-4	16	2.286

X2 = 8.7458

The hypothesis formulated is tested by means of the Chi-square.

The chi-square is 8.7458, which shows that the chi square calculated is greater than the chi-square tabulated (3.84). A decision rule is hereby applied. Therefore, "Audit Trails of the Financial Audit of Banking Sector has impact on fraud detection as well as effect on disaster recovery"

**Test of Hypothesis 2 - Question 3 and 4:**

**H02:** Audit Trails on the Financial Audit of Banking Sector does not recover lost transactions.

**Table 4**

RESPONSES	STRONGY AGREED	AGREED	STRONGLY DISAGREED	DISAGREED	TOTAL
Q III	23	18	8	11	60
Q IV	37	10	9	4	60
<b>TOTAL</b>	60	28	17	15	120

$$X^2 = \frac{\sum (o - e)^2}{e}$$

**Table 5**

O	E	O-E	(O-E)2	(O-E)2/E
23	30.0	-7	49	1.63
18	14.0	4	16	1.14
8	8.5	0.5	1	0.11
11	7.5	4.5	20.25	2.70
37	30.0	7	49	1.63
10	14.0	-4	16	1.14
9	8.5	1	1	0.12
4	7.5	-3.5	12.25	1.63

$$X^2 = \underline{10.1}$$

The hypothesis formulated is tested by means of the Chi-square.

The chi-square is 10.10, which shows that the chi-square calculated is greater than the chi-square tabulated (3.84). We herein apply the decision rule. Hence, Audit Trails on the Financial Audit of Banking Sector assist in the recovery of lost transactions and have impact on regulatory compliance

### **Discussion and Findings**

An audit trail is a useful aid in uncovering fraud in a banking organization. It provides a critical component in fraud detection. Strict adherence to the creation of an audit trail provides information proving the legitimacy of transactions. In addition to recording the metadata behind each individual transaction at the time it was created, an audit trail also records data about transactions that users have edited. All banking transactions (receipts and payments) must have a supporting document such as purchase orders, approved invoices, initiating documents and approvals/authorizations. A bank reconciliation, performed by someone other than the cheque writers and signatories, comprises part of an audit trail. Thus, the audit trail report exposes an individual who accesses the system to alter transactions after other users entered them accurately. The presence of an audit trail requirement not only helps detect fraud, but serves to prevent it. Employees who know that management monitors and tracks their work see less opportunity for fraudulent activity. Audit logs provide objective evidence to support the action an organization takes when it uncovers fraud. If a disaster makes all the transactions for an entire day unavailable, an audit trail report for the day makes it possible to reconstruct corrupt or damaged files. If audit trail logs have been preserved and backed up over a period of time, an audit trail report can recreate an organization's transactions for the entire period. Reconstruction can be a tedious, time-consuming process and may require special software, but if there is no alternative for recovering transactional information, the process is worth the investment.

A carefully crafted blend of procedures, policies, and workflows, internal controls are designed to improve compliance, ensure accuracy in financial statements, and reduce risk. When they are clearly written, provide reasonable contingencies for potential challenges (e.g., computer system problems, human error, process improvement opportunities), and allow for necessary adjustments as circumstances warrant, internal controls can make every aspect of procurement, compliance, and financial reporting, including audit logs, much simpler. Audit Trails provide security-related objectives, individual accountability, reconstruction of events, intrusion detection, and problem analysis, summarized as: Prevention of fraud; Stress-free audits; Better positioned to secure investment and/or loan; Error correction and time-saving; Avoiding regulation compliance infractions. Most organizations are subject to regulations. The Banking and Finance sector in Nigeria is regulated primarily by the Banks and Other Financial Institutions Act (BOFIA), Central Bank of Nigeria Act; the Companies and Allied Matters Act (CAMA); the Nigerian Deposit Insurance Corporation Act (NDICA); the Foreign Exchange (Monitoring and Miscellaneous Provisions) Act; the Financial Reporting Council of Nigeria Act; there is the Regulatory Framework for the Use of Unstructured Supplementary Service Data (USSD) in the Nigerian Financial System; the Revised Standards on Nigeria Uniform Bank Account Number (NUBAN) Scheme for Banks and Other Financial Institutions; Cybersecurity. The CBN also issued a letter to all banks and Payment Service Providers (PSPs) on the Issuance of Risk-Based Cyber-Security Framework and Guidelines for Deposit Money Banks and Payment Service Providers for the DMBs and PSPs to protect and strengthen their cyber security against sophisticated cyber threats. These cyber security threats such as phishing attacks, ransomware, have increased alarmingly due to the use of information technology to expedite transactions. It sets out the minimum cybersecurity to be used by the DMBs and the PSPs to include a cybersecurity strategy/framework, cybersecurity risk management system, and cyber resilience assessment, creation of a cybersecurity profile, metrics, monitoring & reporting processes. This is all to protect confidentiality and prevent financial loss or reputational damage. The issuance of Corporate Governance and Internal Control Codes (the Codes). The Anti-Money laundering Act in conjunction with

the Nigerian Financial Intelligence Unit (NFIU) issue periodic thresh-hold limits and Suspicious Transaction Reports (STPs. The CBN Anti-Money Laundering and Combating the Financing of Terrorism (Administrative Sanctions) Regulations (the "Regulation") is the collaboration effort of the CBN and the Office of the Attorney General of the Federation for an administrative sanctions regime for financial institutions under the supervision of the CBN. The Regulation outlines forty eight (48) actions required for anti-money laundering and combating the financing of terrorism (AML/CFT) for banks and other financial institutions and as well as the administrative sanctions for default. An audit trail report demonstrates compliance with these regulations and helps a company fulfill its record-keeping requirements for compliance purposes and secure the robust financial system.

#### **CONCLUSION AND RECOMMENDATIONS**

The audit trail is an important concept, and has very practical implications. It is a widely researched topic, but in practice many Information Technology (IT) setups lack sufficient audit trail capabilities, mainly because the risks are not immediately obvious, and partly because it is a technically challenging task. Audit trails have transitioned from manual to automated electronic logs that make this historical information more accurate, readily accessible, and usable. Successful audit trails demand a top down commitment by upper management, affected departments, and information technology (IT) personnel. If one knows nothing about a transaction except the day that someone entered it, an audit trail report can help you find the transaction. By reviewing the audit logs for that day and matching them to the transactions one already knows about. It can eliminate the known transactions and find the lost one. The type of accounting software in use determines the steps one takes to find lost transactions. Some applications can search by amount, by transaction number or by the user who entered the transaction. The study recommends that every Organization needs Audit trails. They all need secure and immutable records of where and when a transaction was performed accurately and truthfully. Organizations mostly need these audit trails to comply with industry requirements or government regulations. However, a well-kept audit trail can also help organizations understand the state of their business both past and present. A good audit trail system will enables organizations to, Be compliant with the law or standards, gives a big picture of the business, troubleshoot issues and cutt down the development costs and time-to-market of the applications.

#### **References**

- ACCA Paper P7 INT. (2009). *Advanced Audit and Assurance*. UK: Kaplan Capital Limited
- Adeniji A. (2004). *Audit and Investigations*. Lagos: Value Analysis Consult
- Ann, S. (2019). *How to Conduct a Fraud Investigation: The Complete Guide*. Ontario: I-Sight, Ottawa
- Bana, J.O. (2007). *The Role of Auditors in Investigation of Fraud*. Nigeria: Unpublished Document
- Petraşcu, D.& Tieanu A. (2014). The Role of Internal Audit in Fraud Prevention and Detection. *Procedia Economics and Finance*, 16 (20) 489 – 497.
- Erin, S.,\_Thomas, J. & Lindblad, M. (2017). *What's included in an Audit Trail and Why It's Important*. UK: London Inc
- Henshaw, G. (2019). Nigeria: Regulatory Summary of 2018 – Banking & Finance.
- Nicholas J. P., Vendetti, J.& Zlaullah, K. M.(2018). *The Importance of Audit Trails for Business Security and Compliances*. Nigeria: Publication Inc