Continuous Auditing Fraud Detection System in Nigerian Tertiary Institution Using Multi-Agent and Data Mining.

Amanze, Bethran.C. Department of Computer Science, Imo State University, Owerri. e-mail: amanzebethran@yahoo.com. +2347062523438.

Onukwugha, Chinwe. G (Ph.D). Department of Computer Science, Federal University of Technology, Owerri.

Etim, Emmanuel, O. Department of Computer Science, Abia State Polytechnic, Aba

Abstract

Data mining is a popular way to combat frauds because of its effectiveness. Data mining is a well-defined procedure that takes data as input and produces output in the forms of models or pattern. Intelligent agents for fraud detection can be applied to many areas. One of these areas is continuous auditing. Continuous auditing is a promising field which can automate the auditing process and provide audit reports on a continuous basis. One of weakness of continuous auditing is the possible management fraud problem. Due to the lack of human intervention, management frauds are more likely to occur. A multi-agent system for fraud detection will solve this problem. Agents will deploy in supply chain partners’ sites, at the institution’s general ledger level, and at the institution’s financial statement level. The agents at the partner’s sites can monitor the transaction activities. And they will also interact with general ledger level agents to verify the data accuracy, if there is some unusual transaction, these partner site agents will signal an alarm. After a transaction is completed, all the transaction data will be collected by the general ledger level agents and then delivered to the financial statement level agents. After the delivery, the financial statement level agents will summarize the information will create a set of financial statements. Then agents will compare the data in the reports with those in historical financial reports to check the overall reasonableness. If the data are suspicious, the agents at the financial statement level will alert the human auditor. All these agents will be created and deployed by the institution firms to ensure the auditor’s independence. The agents at the general ledger level and the financial statement level should be at institution-complaint. With the agents’ aid, analytical procedures, substantive tests of balance, and the test of details of balances can be performed automatically. The financial data are double-checked, both with historical data and with partner’s information, to prevent management fraud.
1.0 Background of the study

Across organizations and industries, while the definitions may vary, the goal of CA/CM is to provide greater transparency into the operations and timely reporting of concerns. Continuous auditing consists of the automated collection of audit evidence and indicators by an internal or external auditor from an entity’s IT systems, processes, transactions, and controls on a frequent or continuous basis. This information enhances auditor capabilities and helps to ensure compliance with policies, procedures, and regulations. In many cases, CA can act as an early warning system to detect control failure on a timelier basis than under traditional approaches. In contrast, continuous monitoring is an automated feedback mechanism for management to ensure that the systems and controls have been operating as designed and transactions are processed appropriately. Management can utilize this information to set business rules or tests, using analytics to identify performance gaps or unusual transactions that may suggest control failures. CM allows management to have greater visibility into the organization—enhancing capabilities and entity-level controls while maintaining optimal performance. A CA/CM model integrates management’s responsibility to monitor risk and internal control performance with how the internal/external auditor needs to provide a risk-based level of assurance over management’s controls and monitoring capabilities. Management’s control portfolio includes any number of automated and manual controls designed to mitigate risk and depending on the extent controls are automated, or could be automated, the greater the benefit of providing continuous transparency into performance. For highly manual processes, transactions management, and internal audit, one can utilize macro-level analysis to monitor risks. CA/CM is an ongoing process for both management and the auditors to continuously assess evolving risks, design controls, and implement corrective actions and other changes as necessary. Continuous auditing is an automatic method used to perform auditing activities, such as control and risk assessments, on a more frequent basis. Technology plays a key role in continuous audit activities by helping to automate the identification of exceptions or anomalies, analyze patterns within the digits of key numeric fields, review trends, and test controls, among other activities. The "continuous" aspect of continuous auditing and reporting refers to the real-time or near real-time capability for financial information to be checked and shared. Not only does it indicate that the integrity of information can be evaluated at any given point of time, it also means that the information is able to be verified constantly for errors, fraud, and inefficiencies. It is the most detailed audit. Each
instance of continuous auditing has its own pulse. The time frame selected for evaluation
depends largely on the frequency of updates within the accounting information systems. Analysis
of the data may be performed continuously, hourly, daily, weekly, monthly, etc. depending on
the nature of the underlying business cycle for a given assertion. The objective of financial
reporting is to provide information that is useful to management and stakeholders for resource
allocation decisions. For financial information to be useful, it should be timely and free from
material errors, omissions, and fraud. In the real time economy, timely and reliable financial
information is critical for day-to-day business decisions regarding strategic planning, capital
acquisition, credit decisions, supplier partnerships, and so forth. Advances in accounting
information systems such as the advent of enterprise resource planning (ERP) systems have
enabled the generation of real time information. However, the practice of traditional auditing has
not kept pace with the real time economy. Traditional manual audit procedures are labor and
time intensive, which limits audit frequency to a periodic basis, such as annually. These time and
effort constraints can be alleviated through the use of technology and automation. Continuous
auditing enhances the delivery of auditing services by making the audit process more efficient
and effective through the use of technology and automation. The increased efficiency and
effectiveness of the audit process enables more frequent or real time audits and hence enhances
the reliability of the underlying information (Vasarhelyi, 2011).

2.0 OBJECTIVES OF THE STUDY

(1) Delivering regular insight into the status of controls and transactions across the global
enterprise.
(2) Enhancing overall risk and control oversight capability through early detection and
monitoring.
(3) Using automation to efficiently test a broader range of transactions and controls.
(4) Reporting value to your board and High-level management.

3.0 The Roles of Internal Auditing and Management
Management has the primary responsibility for assessing risk and for the design, implementation,
and ongoing maintenance of controls within an organization. The internal audit activity is
responsible for identifying and evaluating the effectiveness of the organization’s risk
management system and controls as implemented by management. Auditors conduct the evaluation to provide assurance to the audit committee and senior management as to the state of risk and control systems and, in the case of legislation such as the Sarbanes-Oxley Act, the reliability of management’s representation concerning the state of controls. Ideally, internal auditing is not part of the controls monitoring process and does not design or maintain the controls, thereby retaining its independence.

Although the monitoring of internal controls is a management responsibility, the internal audit activity can use and leverage continuous auditing to strengthen the overall monitoring and review environment in an organization.

The level of proactive monitoring performed by management will directly affect how auditors approach continuous auditing. In cases where the continuous monitoring of controls is being performed by management, the same level of detailed transaction testing may not be required under continuous auditing. Instead, auditors can focus on procedures to determine the effectiveness of management’s monitoring process and, depending on the outcome of such tests, adjust the scope, number, and frequency of audit testing.

4.0 Continuous Monitoring

Continuous Monitoring is a process that management puts in place to ensure that its policies, procedures, and business processes are operating effectively. Management identifies critical control points and implements automated tests to determine if these controls are working properly. The continuous monitoring process typically involves the automated testing of all transactions and system activities, within a given business process area, against a suite of controls rules. The monitoring typically is put in place on a daily, weekly, or monthly basis, depending on the nature of the underlying business cycle. Depending on the specific control rule and the related test and threshold parameters, certain transactions are flagged as control exceptions and management is notified. The management monitoring function may also be tied to key performance indicators (KPIs) and other performance measurement activities. It is management’s responsibility to respond to the monitoring alerts and notifications and to remediate any control deficiencies and correct defective transactions (Van, 2004).
5.0 Continuum of Continuous Auditing

Continuous auditing helps auditors to identify and assess risk, as well as establish intelligent and dynamic thresholds that respond to changes in the organization. It also supports risk identification and assessment for the entire audit universe, contributing to the development of the annual audit plan, as well as the objectives of a specific audit. As such, continuous auditing can be seen as a continuum operating on many levels. Also, different points on the continuum are better suited to different tasks, and it is possible to be at more than one point on the continuum as you perform different tasks. The focus of continuous auditing ranges from controls based to risk-based analysis techniques range from the real-time review of detailed transactions to the analysis of trends and comparison of entities against other entities and over time. At the “controls” end of the continuum, related audit activities include control assurance and financial attest audits.

1. As you move to the other end of the continuum, audit activities include the identification of fraud, waste, and abuse through to the assessment of risk to support audit projects and to produce the annual audit plan.

2. Related management activities include continuous controls monitoring, performance monitoring, balanced scorecard, total quality management, and ERM.

Continuous auditing is a unifying structure or framework that brings control assurance, risk assessment, audit planning, digital analysis, and the other audit tools, techniques, and technologies together. It supports micro-audit issues, such as detailed transaction testing to assess the effectiveness of controls, and macro-audit issues, such as using risk identification and assessment to prepare the annual audit plan. It also addresses the mid-level requirements, such as the development of audit objectives for individual auditing (Vasarhelyi, 2011). The main difference between the micro- and macro audit levels is the granularity of the information required:

1. Control testing requires detailed information — down to transactions at the source level. Continuous control assessment uses carefully developed rules and real-time, or near real-time, testing of transactions for compliance with these rules.

2. Individual auditing often starts with the risks identified in the annual audit plan but uses more detailed data analysis and other techniques (e.g. interviews, control self-
assessments, walkthroughs, questionnaires, etc.) to further define the main areas of risk and focus the risk assessment and subsequent audit activities.

(3) The annual audit plan requires high-level information — perhaps several years’ worth of data — to establish the risk factors, prioritize risks, and set the initial timing and objectives for the planned set of audit.

5.1 Components of continuous auditing

Continuous auditing is made up of three main parts: continuous data assurance (CDA), continuous controls monitoring (CCM), and continuous risk monitoring and assessment (CRMA) (David, 2011).

Continuous Data Assurance

Continuous data assurance (CDA) verifies the integrity of data flowing through the information systems. Continuous data assurance uses software to extract data from IT systems for analysis at the transactional level to provide more detailed assurance. CDA systems provide the ability to design expectation models for analytical procedures at the business-process level, as opposed to the current practice of relying on ratio or trend analysis at higher levels of data aggregation. CDA software can continuously and automatically monitor transactions, comparing their generic characteristics with predetermined benchmarks, thereby identifying anomalous situations. When significant discrepancies occur, alarms are triggered and routed to appropriate stakeholders and auditors.

Continuous Controls Monitoring

Continuous controls monitoring (CCM) consists of a set of procedures used for monitoring the functionality of internal controls. CCM relies on automatic procedures, presuming that both the controls themselves and the monitoring procedures are formal or able to be formalized. CCM can be used for monitoring access control and authorizations, system configurations, and business process settings. CDA and CCM are complementary processes. Neither process is self-sufficient or comprehensive. Even if no data faults are found it cannot be concluded that controls are fail-
safe. Further, even if controls are being implemented, data integrity cannot be assumed. When combined, however, these monitoring approaches present a more complete reliance picture.

Continuous Risk Monitoring and Assessment

Continuous risk monitoring and assessment (CRMA) is used to dynamically measure risk and provide input for audit planning. CRMA is a real-time integrated risk assessment approach, aggregating data across different functional tasks in organizations to assess risk exposures and provide reasonable assurance on the firms’ risk assessments.

6.0 Methodology

A multi-agent system for fraud detection will solve this problem. Agents will deploy in supply chain partners’ sites, at the institution’s general ledger level, and at the institution’s financial statement level. The agents at the partner’s sites can monitor the transaction activities. And they will also interact with general ledger level agents to verify the data accuracy, if there is some unusual transaction, these partner site agents will signal an alarm. After a transaction is completed, all the transaction data will be collected by the general ledger level agents and then delivered to the financial statement level agents. After the delivery, the financial statement level agents will summarize the information will create a set of financial statements. Then agents will compare the data in the reports with those in historical financial reports to check the overall reasonableness. If the data are suspicious, the agents at the financial statement level will alert the human auditor. All these agents will be created and deployed by the institution firms to ensure the auditor’s independence. The agents at the general ledger level and the financial statement level should be at institution-complaint. With the agents’ aid, analytical procedures, substantive tests of balance, and the test of details of balances can be performed automatically. The financial data are double-checked, both with historical data and with partner’s information, to prevent management fraud.

Conclusion

In light of today’s challenges, it is imperative that CAEs find new ways to enable the internal audit function to respond effectively to the demands of a rapidly changing business environment and the burden of growing regulatory compliance requirements. The integrated approach of
continuous auditing and continuous monitoring, enabled by technology, is the key to a sustainable, cost-effective, and resource-efficient solution. These challenges can be viewed as an opportunity for the internal audit profession and its leaders to provide tremendous value to the organization. Internal auditing is uniquely positioned to not only provide the organization with assurance that it is in compliance with laws and regulations, but also to assist the organization in improving the effectiveness and efficiency of business processes. The return of implementation of continuous auditing will be realized through improvements to an organization’s bottom-line results, based on the timely identification of errors, fraud, and the creation of a stronger internal control environment across the enterprise.

References


Glen L.Gray and Maryann,J. Gray (2000) “Assuranc services within the auditing profession” The IIA Research foundation, Ailamonte springs, fla; USA.


