NET WORK OF INTERNAL AUDIT FUNCTION AS A MANAGERIAL ANALYTICAL TOOL

ThankGod C Agwor, Dr

Available at: https://works.bepress.com/thankgod_agwor/6/
NET WORK OF INTERNAL AUDIT FUNCTION
AS A MANAGERIAL ANALYTICAL TOOL

By

TIANKGOD C. AGWOR
Department of Accounting
Rivers State University of Science and Technology
Port Harcourt

And

AMA G. A. NDUKWE
Department of Accounting
Abia State University,
Uturu

ABSTRACT

The paper examines the network of internal audit function and revealed how it is used as a managerial analytical tool in the use of human and economic resources at the workplace. The major highlights of the paper are divisionalization and distinct programming of auditing activities, including the steps in process control. The paper also revealed measures for safeguarding human and economic assets. It drew attention to the implications of internal audit function in the management of fraud.

INTRODUCTION

The internal audit function has been described by a host of researchers as an independent appraisal activity within an organization for the review of operations and as a service to management (Adams, 2005; Starling, 1979). Internal audit function is an independent appraisal operations established by management. It evaluates and reports on the adequacy of internal control as a contribution to proper economic, effective and efficient use of
organizational resources. According to the Institute of internal Auditors professional practices framework, internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and corporate governance. This definition reflects the changing role of internal auditors. Internal auditors are expected to provide value to the organization through improved operational effectiveness, in addition to traditional responsibilities such as reviewing the reliability and integrity of information, compliance with policies and regulations, and the safeguarding of assets.

INDEPENDENCE OF AUDIT FUNCTION
There has been emphasis on independence in auditing because it is seen essentially as, characterized by interruption of its intended objective approach to work. Woolf (2003) refers to this independence and auditing as the twin sides of the same coin. The author explained that, independence is a major attribute enabling the auditor to ensure accountability. Woolf (2003) argued that a dependent auditor is a contradiction of terms, because if an auditor is dependent, the essence of his appointment is completely lost. In the same way, Stamp (1998) has advanced the argument that if the auditor is not independent, then the sole justification of his existence disappears.

Akpa (2007) argued that, an internal auditor should always maintain, under all circumstances, a great sense of personal integrity and the will to act objectively even in the tce of intense pressurt

Whether in private or public practice, he is expected to remain independent both in fact and in appearance before those he serves. The objectives of internal auditors are considerably broader than the objectives of external auditors. This provides
flexibility for internal auditors to meet company needs. Different companies vary in the extent of internal auditing and the areas on which require the internal auditors focus. For instance, management of one company may decide that internal auditors should evaluate the internal controls and financial statements of every division, annually. Whereas others may decide that the internal auditors should serve primarily as consultants and focus on recommendations that will improve organizational performance (Soyode, 2001) Abiola (2003) argued that the purpose of internal audit is to evaluate and discover the reasons for successes and failures, also to identify the key success factors for the future. In performing internal audit, the planners will heavily rely on the experience of other corporate organizations, their own strength and weaknesses and compare these strength and weaknesses, to the key success indicators of other organizations in the same industry. According to Abiola (2003), internal audit also covers the process of giving reports, defending decisions and actions taken for the responsibility received for managing organization’s or public resources with or without laid down guidelines and procedures.

Lemon (1988) has advanced that the two most important qualities of an operational auditor are independence and competence. Who the auditor reports to is important to ensure that investigation and recommendations are made without bias. The responsibilities of operational auditors also affect their independence. The internal auditor should not be engaged in the performance of operating functions in a company or for correcting deficiencies, where ineffective or inefficient operations exist. For instance, it would negatively affect auditors’ independence, if they were responsible for designing an electronic data processing system for purchases or for
correcting it, if deficiencies were found during an audit of the purchasing system. It is acceptable for auditors to recommend changes in operations, but operating personnel must have the authority to accept or reject the recommendations. If auditors had the authority to require implementation of their recommendations, the auditor would, in essence, have the responsibility of auditing his or her own work the next time an audit is conducted. Independence would be reduced rendering internal audit ineffective (Arens 2003, Loebbecke, 2000).

DIVISION AND PROGRAMMES
Anders (2003) suggested the division of internal audit into four categories, based on the objective or techniques of the audit. These are: (1) system based audit; (2) financial or accounting audit; (3) performance or operational audit and (4) compliance audit which also includes regulatory and programme audit. It appears therefore, that the system based audit refers to an in-depth evaluation of the internal control system with the objective to assess the extent to which controls are functioning effectively. Functional audit concentrates on establishing compliance with appropriate laws and determination of whether functional reports prepared are accurate and reliable. It also covers checks or occurrences of embezzlement. Management and operations audit focuses on efficiency of operation, including utilization and control of resources, wastages rather than theft (Anders 2003). Programme audit is a check on whether the objectives of the programme are being met, a confirmation or otherwise of desired results achievement. In certain situations internal auditing and operational auditing are interchangeably used, because of the uniqueness and close relationship of both expressions. It is, however, inappropriate to conclude that all operational auditing is done by internal auditors or that internal auditors do only operational auditing. Many internal audit departments do both operational and financial audits. Often the two audits are done simultaneously. The unique
advantage internal auditors have, in doing operational audits is that they spend all of their time working for the company they are auditing. They thereby develop considerable knowledge about the company and its business, which is essential to effective operational auditing.

Lemon (1988) argued that the internal audit department should report to the board of directors or president/Chief Executive Officer. Internal auditors should also have access to and ongoing communications with the audit committee of the board of directors. This organizational structure helps internal auditors remain independent if internal auditors were to report to the controller, it would be difficult for the internal auditor to independently evaluate and make recommendations to senior management about inefficiencies in the controller’s operations. Performance audit, which can result to closing down or termination of ineffective agencies or programmes, assesses the total operations of an entity.

The areas covered by this audit type include compliance, management, programme and regulatory audits. Therefore, these are responsible to a large extent why, Millichamp (1986) defines internal auditing as an independent appraisal function within organization for the review of system of control and quality of performance, as a service to the organization. It objectively examines, evaluates and reports on the adequacy of internal control to the proper economic, efficient and effective use of resources.

This appears to corroborate the view of the Institute of Chartered Accountants of England and Wales (ICAEW) which defined internal auditing as a review of operations and records, sometimes continuous, undertaking within a business by specially assigned staff. Viewing this critically, Tocki (1979) extracted four principal facts from the definitions namely, that: (1) internal audit is an internal function, which means that, it is conducted by the employees of an organization, specially assigned for this purpose; (2) the internal auditor’s function is to review and appraise an organization’s operations and records; (3) internal audit is a service to management, consequently, the scope and objectives depend upon management’s assessment of what is needed and
its willingness to assign the task to the internal auditor; and
(4) internal audit being a review and appraisal function to be
conducted effectively, the auditor requires the status of
independence.
From the foregoing, it can be argued that the purpose of
internal auditing is not to discover fraud and other kinds of
misdemeanor in business processes. Therefore, properly
conducted internal audit may reveal discrepancies, mistake,
loop-holes in the system and fraudulent manipulations. This
does not mean that ny internal audit work that did not reveal
discrepancies is not properly conducted, as such
discrepancies can only be discovered, where they exist. Having
operationalized the concept of internal audit function, the key
components or dimensions that emerged are process control,
assets safeguard and fraud prevention which are discussed
below.
A1JDIT PROCESS CONTROL
It has been acknowledged that, some of the hallmarks from
the assessment of the nature of internal audit function, relates
to the internal auditor as requiring independence; sound
judgement and transparency, we shall therefore, evaluate
process control as one of the measures of internal audit
function. A process is a sequence of steps taken to achieve a
goal. In industry processes are sequences of steps taken to
produce goods and services.

According to Creswell (1994) ideally, a model also yields
accurate predictions of the future behaviour of the process.
Therefore, model can be used as a basis for process control.
Control may mean keeping the process outcomes near a
predetermined target so that the output from the process is
dependable. This type of control, which is also referred to as
process regulation, is typical in manufacturing, agriculture
and other management applications.
A major control available in a small company is the knowledge
and concern of the top operating person, who is often an
owner-manager. A personal interest in the organization and
close relationship with personnel make careful evaluation of
the competence of the employees and the effectiveness of the
overall system possible. For instance, internal control can be significantly strengthened if the owner conscientiously performs such duties as signing all cheques after carefully reviewing supporting documents, reviewing bank reconciliations, examining accounts receivable statements sent to customers, approving credit, examining all correspondence from customers and vendors, and approving bad debts.

How large or small an organization is, has a significant effect on the nature of internal control and the specific controls that are placed in operation. Obviously, it is more difficult to establish adequate separation of duties in a small company. It would also be unreasonable to expect a small firm to have internal auditors. However, if the various subcomponents of internal control are examined, it becomes apparent that most are applicable to both large and small companies. Even though it may not be common to formalize policies in manuals, it is certainly possible for a small company to have (1) competent, trustworthy personnel with clear lines of authority; (2) proper procedures for authorization, execution, and recording of transactions; (3) adequate documents, records, and reports; (4) physical controls over assets and records; and, to a limited degree and (5) independent checks on performance.

**HUMAN AND ECONOMIC ASSETS SAFEGUARD**

We have in the previous section discussed that process control, as a measure of internal audit function, stipulates measure and procedures necessary for regulating organisational members in strategy implementation. However, in this section, we shall examine assets safeguard which is another measure of internal audit function. An asset is an economic resource or property belonging to a person or business organization. It consists of plants, buildings, machinery, motor vehicles, representing fixed assets, delil ors, casl, and sick which are of three categories: finished goods, work—ui—progress and raw materials representing current assets, then goodwill, patent and copyrights representing hclilious or intangible assets and coal, barites, gypsum, tin
and other solid minerals, represent wasting assets (Meigs et al., 1993, Igben, 2004, Adams, 2005). According to Pandey (1995), the recognized major forms of stock are raw materials, work-in-progress that facilitates production and stock of finished goods, required for smooth marketing operations. Physical safeguards are necessary for records and documents. The redevelopment of lost or destroyed records is costly and time consuming. Imagine what would happen if an accounts receivable master file were destroyed. The considerable cost of backup records and other controls can be justified to prevent this loss. Similarly, such documents as insurance policies and notes receivable should be physically protected (Arens 2003). Mechanical protective devices can also be used to obtain additional assurance that accounting information is currently and accurately recorded. Cash registers and certain types of automatic data-processing equipment are all potentially useful additions to the system of internal control for this purpose. Lemon (1988) argued that the most important type of protective measure for safeguarding assets and records is the use of physical precautions. An example is the use of store rooms for inventory to guard against theft. When the storeroom is under the control of a competent employee, there is further assurance that obsolescence is minimized. Fireproof safes and safety deposit vaults for the protection of assets such as currency and securities are other important physical safeguards.

There are three categories of controls related to safeguarding Information technology equipment, program and data files. As with other types of assets, physical controls are used to protect the computer facilities. Examples are locks on doors to the computer room and terminals, proper control of environmental conditions such as temperature and humidity in the computer room, adequate storage space for software and data files are useful to protect them from less, and proper fire-extinguishing systems. Access controls deal with ensuring that only authorized people can use the equipment and have access to software and data files. An example is an online access password system. Backup and recovery procedures are
steps an organization can take in the event of a loss of equipment, programs, or data. For instance, a backup control of programs and critical data files stored in a safe, remote location, is a common backup control.

In an electronic data processing system, any person with custody of assets should be prevented from performing the programming function, and have read only access to terminals. As a general rule it is desirable that any person performing an accounting function, relating to transactions should hold a position commensurate with the nature and significance of the transactions. The policy for such authorizations should be established by top management. For instance, a common policy is to have all acquisitions of capital assets over a set amount authorized by the board of directors or the acceptable relevant authority (Aboyade 2005).

Libby et al (2002) argued that there is also a distinction between authorization and approval. According to them authorization is a policy decision, for either general transactions or specific transactions while approval is the implementation of management’s general authorization decisions. For instance, assuming management sets a policy, authorizing the ordering of inventory when there is less than a three-week period supply on hand, that is regarded as general authorization.

ANNEX OF FRAUD PREVENTION

In our previous discussion on assets safeguard, it was established that internal audit involves the responsibility of guarding against unwarranted loss of asset. In this section we are going to examine fraud prevention as a related measure to assets safeguard. Marshal (2000) defined fraud as obtaining a material advantage by unfair action. The Canadian Institute of Chartered Accountants CICA (1981) referred to fraud as acts committed with an intent to deceive, involving either misappropriation of assets or misrepresentations of financial information, either to conceal misappropriation of assets or for the purpose of such means as manipulation, falsification or alteration of records, or documents, suppression of
information, transactions or documents and misapplication of accounting principles.

Radburn (1982) while examining the delinition ol fraud by the American Business Association, described fraud as any non-violent, illegal activity which principally involves deceit, misrepresentation, concealment, manipulation, breach of trust, subterfuge or illegal circumvention. Thus, we can generally subscribe to a more simplified argument that fraud is a wrongful, non violent act with the intent to deceive and cheat. The issue of fraud has become ‘food for thought’ for many corporate bodies in recent times. In an attempt to proffer solutions to the persistent fraudulent practices among Management and their Subordinates, a greater part of time spent in board meetings is devoted to the menace of fraud. The frequency of occurrence in any establishment tends to determine the long term survival and growth of the organization. Therefore if it is not handled with due care, it could lead to corporate failures.

Abdullahi (2007) defined fraud as any intentional distortion of financial statements and other records and the misappropriation of assets. This may involve falsification or alteration of accounting records or other documents, suppression or omission of the effects of transaction from records or documents, willful misrepresentations of transactions or of organization’s state of affairs, and recording transactions which have no substance. Fraud embrace a very wide spectrum of deceptive and illegal behaviour that may be encountered and goes by many names that are included in wrongdoing by deceit such as white-collar crime and embezzlement. It is not restricted to monetary or material benefits; it covers other areas such as the obtaining of status, or access to information by dishonest means and for dishonest purposes. Fraud and irregularity therefore cover the intentional distortion of financial records, either to conceal the misappropriation of assets, or for some other purpose.

Abdullahi (2007) argued that there are many reasons for the increasing fraudulent practices in the publicly owned quoted companies. Fraud is becoming more attractive to organized
criminals, because of the impression that it is low risk/high reward especially when compared to other crimes against individuals or corporate organisations. A great deal of fraud is not committed by professional fraudsters, but by ordinary people who are simply not sufficiently motivated to overcome inertia and comply with requirement. With the increased use of information technology in the function of publicly owned quoted companies, the perpetration of fraud has become more sophisticated and detection of fraud has been made more complicated. Fraud thrives, when an organisation’s internal control system are weak.

According to Pius (2007) some of the common causes of fraud in Nigeria can be grouped into two broad categories: individual and institutional causes. The individual causes include: low value system, peer group pressure, greed, extended family relationship or dependency Syndrome, family background, and hereditary values. Whereas the institutional causes include weak rules and sanctions. Low salary, promotion unconnected to performance, centralization of government functions, bureaucracies, lack of protection for those who expose and resist fraud. The impact of fraud Weakens institutional capacity and erodes public confidence.

Fraudulent practices lead to increased prices of goods, services and higher taxes. The sheer scale of some frauds can undermine the corporate policy objectives and the confidence of work force in organization. The effect of fraud is noticeable in government non delivery of essential services, increase in tariffs and taxes, poverty, crime, rate of disease, unemployment, and disposable income, dysfunctional household and decline in economic activity. Fraud can also have a detrimental effect on the individuals. Work groups can be severely disrupted during investigations, resulting in lowered morale and reduced productivity and even interference with the private lives of innocent individuals. Consequently, threaten the wellbeing of an organization, through the harm done to its organizational fabric and the damage inflicted on personal relationships.

Okoye (2007) while analyzing the behaviour theory of fraud argued that Fraud has become one of the greatest threats to
the world economy. It is a global problem, not only in terms of its impact on our major corporations and key financial institutions, but also its effect on smaller companies and ultimately the wider public who indirectly pay for the losses through increased costs of goods and services. Okoye (2007) argued that, many organisations seem to have failed to recognise that fraud can prove to be even more catastrophic than other forms of critical incidents such as terrorist attack, fire or flood. Events of that nature may cause serious disruption to businesses but rarely are they insurmountable. However, a significant fraud against a company not only undermines financial stability, it can ultimately result in such damage to the reputation and loss of investor’s confidence that it proves irrepairable.

It is often for these reasons that some company directors write off losses to fraud, under the general heading of Bad Debt rather than admit that there has been a failure to implement proper safeguards or managerial negligence in applying appropriate levels of oversight to routine business and assets are place at risk. It can be very difficult to judge the level of fraud from statistics based on prosecutions, convictions or even reports to the police on fraud, because there is a large number of cases that goes unreported. Companies in particular, are not always keen to report fraud for fear of the repercussions it may have on their business. This may include trading partners being less willing to use the company, investors not wishing to invest in the company and a general fall in the company’s reputation.

CONCLUSION AND IMPLICATIONS FOR MANAGEMENT OF FRAUD

There is no denying the fact that fraud has become a recognized institution in the national and international financial system, and fraudsters through their show of affluence are well respected in the society and consequently treated as heroes, instead of villains. The implication of this is that hoards of companies are now faced with the arduous task of how to control and minimize the cankerworm. Perhaps, it could be argued that some boards have not done enough, in terms of putting an active preventive mechanism in their
administrative and internal control procedures, as a countermeasure to ward off the persistent fraud syndrome in the financial system. The manner with which fraudsters have continued to carry out their nefarious activities, is a sure indication of serious weaknesses in the internal control systems of most of our corporate entities. Fraud is preventable from the onset (ab initio), but when there is eventual or incidental suspicion, it may then be investigated and ultimately detected, where it actually existed or occurred.

In many business organizations the issue of fraud is often relegated or handled with disdain. If the trend is left unchecked, may lead to economic downturn in business operations (Wells, 2005). According to Penny (2002), sixty three percent (63%) of fraud cases, occur because controls are not operated as set out in the organisations’ policies. It is equally known that some organizations that are facing serious fraud cases have adequate internal control systems. It implies that adequate internal control systems will not bring permanent solutions to problems associated with fraud.

Wells (2005) had advanced that internal controls are not enough to fight fraud. But rather suggests the implementation of the behavioural theory of fraud, drawn from the work of psychologist B. 1’ Skinner and others. He equally suggests the adoption of Cressey’s (2005) fraud triangle as a way out of the global impending economic doom championed by fraud. Cressey (2005) concluded that individuals commit fraud when three factors are present: A financial need that cannot be shared, a perceived opportunity for illicit gains or gain improper access to funds, a personal justification of the act to themselves. In other words, people commit fraud because they need or think they need the money, they believe they will not be caught; and they have justified the act to themselves. Cressey (2005) reportedly asked offenders why they had not committed violations at other times and received three basic replies: there was no need for it before this time; the idea never entered my head; and I thought it was dishonest then, but this time it did not seem dishonest.

Cressey’s (2005) ideas have become known as the fraud triangle consisting of perceived opportunity, pressure and
rationalization. Cressey (2005) catalogued six types of non-shareable problems that often lead to fraudulent acts: Inability to liquidate debts, problems resulting from personal failure, business reversals, physical isolation, status gaining, employer-employee relations. Internal auditors perceive that the fraud triangle suggests at least three general ways of preventing fraud: by altering the motives of individuals, by limiting the opportunity for secretly gaining access to funds, and by undermining common rationalizations through general education or interrogation of individuals. Auditors equally perceive that behaviour is learned and can thus be modified. However, they believe that the best deterrent of all is removing temptation from possible offenders.
REFERENCES


