International Journal of Multidisciplinary Education and Research
ISSN: 2455-4588
Impact Factor: RJIF 5.12
www.educationjournal.in
Volume 3; Issue 6; November 2018; Page No. 01-05

Conceptual study of fraud and the accounting system

Md. Abdul Baten
Brentwood Open Learning College, United Kingdom

Abstract
The concept of fraud, its antecedents and outcomes as well as its detection and prevention, have been discussed by both academics and practitioners for decades. The effects of crime act upon the economy in two primary ways. Microeconomics deals with the effect on individuals and businesses. Macroeconomics deals with the effect on the local community, national, and international economies. Individuals and businesses can easily understand the effect of crime in their everyday activities. However, most individuals and businesses have difficulty understanding the effect of crime on the community, national, and international levels. This paper provides an overview of the recent evolution of Accounting Information Systems (AIS) and their controls for combatting fraud and misconduct. Many completed and ongoing studies have demonstrated the beneficial impacts of AIS on organizations. These studies also summarize potential threats to AIS from employee and/or management ethical misconduct or attempts to commit fraud. Such threats can result in misrepresentation in Financial Accounting reporting for both external and internal and can have undesirable impacts on the integrity and exactitude of the organization's financial reporting and its overall corporate image.

Keywords: concept of fraud, accounting information systems, combatting, prevention

Introduction

Accounting conceptual framework and accounting scandals

The Conceptual Framework (or "Concepts Statements") is a body of interrelated objectives and fundamentals. The objectives identify the goals and purposes of financial reporting and the fundamentals are the underlying concepts that help achieve those objectives. Those concepts provide guidance in selecting transactions, events and circumstances to be accounted for, how they should be recognized and measured, and how they should be summarized and reported. We know that accounting scandals which arise from intentional manipulation of financial statements with the disclosure of financial misdeeds by trusted executives of corporations or governments. Such misdeeds typically involve complex methods for misusing or misdirecting funds, overstating revenues, understating expenses, overstating the value of corporate assets or underreporting the existence of liabilities. It involves an employee, account or corporation itself and is misleading to investor and shareholders.

Creative accounting can be used to manage earnings, for example. Pressure to meet short-term expectations of year-end financial targets may be a cause of creative accounting activity. Creative accounting consists of accounting practices that follow required laws and regulations, but deviate from what those standards intend to accomplish. Creative accounting capitalizes on loopholes in the accounting standards to falsely portray a better image of the company. Although creative accounting practices are legal, the loopholes they exploit are often reformed to prevent such behaviors. Earnings management occurs when managers use judgment in financial reporting and in structuring transactions to alter financial reports to either mislead some stakeholders about the underlying economic performance of a company or influence contractual outcomes that depend on reported accounting numbers.

A primary benefit of public accounting statements is that they allow investors to compare the financial health of competing companies. However, when firms indulge in creative accounting them often distort the value of the information that their financials provide. Therefore, through accounting control which is the methods and procedures that are implemented by a firm to help ensure the validity and accuracy of its financial statements, creative accounting involving the use of unorthodox techniques to adjust the reported profit level or financial position of a business can be pressed. Of course, the accounting controls do not ensure compliance with laws and regulations, but rather are designed to help a company comply.

Accounting information system (AIS)

In essence, the goal of an accounting system is to record financial data and turn it into useful financial information. An accounting information system is usually run using electronic data processing equipment, but can be operated less efficiently with a manual bookkeeping system. Using a computer-based system is highly advantageous, since it automates many accounting processes and thereby reduces transactional error rates. It can also produce reports much more quickly than a manual system. In core accounting practice, we might face a wide range of errors including those of omission, commission, original entry, reversal of entries among others; which can easily be manipulated with wrong defined steps.

The importance of AIS is vital, given the essentially total

reliance of accounting and auditing on computerized information systems. The information is entered into the system and the system tracks and organizes the accounting information. The accounting information system is used also to provide detailed information about the company, including financial statements. Businesess can improve security by limiting the number of people who can access your system. By doing this, they can ensure that the data remains confidential and data are being secured. Plus, if anything goes wrong, it is easier for you to track down the digital footprints. In addition, limiting the number of people who have access to the system best accomplishes to ensure that the business maintains correct data securely. The leaders of the organization must decide who that will be. For example, trained clerks, bookkeepers or accountants require access to verify and enter data into the system and generate reports. Other associates of the organization, both internal and external, generally have no need to manipulate the data. Therefore, if the system is well computerised, deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right can be mitigated.

Control self-assessment (CSA)

The success of enterprise-wide risk management depends on an integrated process for ensuring that risks are assessed and managed across an organization in a dynamic and meaningful way. There are many techniques for reaching all parts of an organization so that self-assessment by front line staff becomes the norm. Some argue the widespread use of questionnaires that are completed by key employees as a way of assessing whether there are operations that are at risk and whether controls are addressing these risk areas properly. Another technique is the use of interviews with managers in particular business units to gauge whether the area is under control or not. A further approach is to commission comprehensive reviews of risk in high profile parts of the organization normally by the use of external consultants, who would report back on any problems found. These three techniques are fairly straightforward in that they involve a process superimposed on the normal business operations and support services.

The important point to note in this section is the need to allows managers and work teams directly involved in business units, functions or processes to participate in assessing the organization's risk management and control processes as well as engaging in a structured discussion for the purposes of identifying risks and potential exposures to achieving strategic business objectives, determining the likelihood of incurring the identified risks, evaluating the controls tasked with managing or mitigating the risks, and implementing remediation plans to either eliminate, reduce, or transfer the risks. Internal controls are fundamental to any system. Its analysis should involve everyone in the organization in order to benefit from a greater appreciation of control procedures and their importance in achieving your strategic business objectives. CSAs help strengthen the internal control environment, which in turn, heightens the level of assurance for all stakeholders involved.

The power of self-assessment lies in its ability to provide information that would not otherwise be easily obtainable, through the participation of employees who know, better than anyone, what is helping them or stopping them from getting their work done. Addituonally, control self-assessment creates a clear line of accountability for controls, reduces the risk of fraud, (by examining data that may flag unusual patterns of transactions) and lowers risk profile. A number of other soft benefits have been claimed by organisations performing control self-assessments. These include a better understanding of business operations (by both management and operational staff), stronger awareness of risk practices and a reinforced governance regime. An effective and efficient CSA can assist in limiting the need for extensive audit testing and can reduce auditor fatigue and assurance overload.

Embedded risk management

Risk management is made to protect a company or organization that also includes employees, property, reputation and others from of danger that can occur at any time. We can know that not all risks can be eliminated or avoided, therefore preventive actions or actions are needed to deal with the identified risks. In this article we will explain some steps that can be taken in the risk management process to help organizations design and implement an effective and proactive risk management plan.

Risks can come from various sources including uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. There are two types of events i.e. negative events can be classified as risks while positive events are classified as opportunities. Several risk management standards have been developed including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards. These standards are designed to help organizations identify specific threats, assess unique vulnerabilities to determine their risk, identify ways to reduce these risks and then implement risk reduction efforts according to organizational strategy.

Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety. Strategies to manage threats (uncertainties with negative consequences) typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some or all of the potential or actual consequences of a particular threat, and the opposites for opportunities (uncertain future states with benefits). In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss (or impact) and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice the process of assessing overall risk can be difficult, and balancing resources used to mitigate between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Using data analysis to detect fraud

Most frauds are still discovered by outside sources such as police, anonymous letters, and customers. Others are discovered only by accident. This raises questions about the methods auditors are applying to seek out and investigate fraud. To cope with thousands, even millions, of transactions, and pick out the few that may be fraudulent, auditors and fraud investigators need powerful data analysis tools. However, the data analysis techniques that comprise state-of-the-art fraud detection tools can sometimes be perplexing. I hope that by shedding light on these techniques and providing easy-to-use fraud tests, Fraud Detection Techniques Using ACL will help auditors and fraud investigators discover fraud and take measures to prevent it.

The tried-and-true techniques and practices of auditing do not always work. Often a paper trail does not exist and the risks are completely different from those in manual or paper-based systems. For many years auditors and fraud investigators relied upon a manual review of the transactions. Auditors were often depicted with their shirtsleeves rolled up, poring over mountains of paper. For example, it was once standard practice to open the file cabinet and select every fifth file for examination, a technique known as interval sampling.

Today, however, more and more fraud auditors are making automated tools and techniques a part of their investigations. Data analysis software allows investigators to gain a quick overview of the business operations and easily drill down into the details of specific areas. As a result, examinations are much more detailed and comprehensive than a manual review of a sample of files. Computer-assisted audit techniques can be used to develop an understanding of the relationships between various data elements, both financial and nonfinancial, and to examine the data for trends. Analytical procedures can be used to perform substantive tests and conduct investigations. Computers not only provide analytical opportunities, but also aid in the understanding of the business area and its associated risks.

Identified control weaknesses must be examined from the point of view of who can benefit. Without a clear understanding of the control weakness, and an assessment of who could take advantage of the weakness, auditors are still somewhat in the dark. Assessing the degree to which people could benefit from the weakness gives you a measure of "opportunity." The fraud triangle-opportunity, rationalization, and pressure-is what drives people to commit fraud. The understanding of who could exploit the identified control weakness can focus the search for fraud on the persons with the greatest opportunity to commit the fraud.

Computer-assisted audit techniques can be used to develop an understanding of the relationships between various data elements, both financial and nonfinancial, and to examine the data for trends. Analytical procedures can be used to perform substantive tests and conduct investigations. Computers not only provide analytical opportunities, but also aid in the understanding of the business area and its associated risks. Identifying risks and measuring losses electronically can improve the overall quality of a fraud investigation. Results can help fraud investigators focus their efforts and address areas of abuse and fraud, rather than waste time reviewing valid transactions.

Patterns can also serve as auditor-specified criteria. Transactions meeting the criteria can trigger automatic investigations. Ideally, the data patterns are used to develop a "fraud profile" that gives fraud investigators a way to detect fraud early in its life cycle. An understanding of how the fraud occurs, and what it looks like in the data allows investigators to search the data for the symptoms of fraud. Depending on the degree of risk, analyzing data for fraud symptoms can be a monthly, weekly, or even daily event.

Systems can also be built for the continuous auditing of transactions to compare them with the fraud profile. One example is the use of cardholder profiles by major credit card companies. Each purchase by every cardholder is compared to the cardholder's normal pattern of purchases. The analysis uses known symptoms of possible frauds, such as two purchases on the same card within hours of each other from stores that are thousands of miles apart. Continuous monitoring also tracks and compares patterns in the data, that is, typical dollar value of purchases, types of purchases, and even the timing of the purchases. Thus, cardholders can be called to verify purchases on their cards minutes after the purchases are made. The aim? To prevent the use of stolen cards, even when the cardholders have not yet reported their loss.

Deterring fraud by increasing risk of detection

Perhaps the most significant objective of proactive fraud investigation is the internal control effect that it establishes, if done properly. Regardless of how unsuccessful a proactive fraud examination may be in detecting fraud indicia, it can always serve as a deterrent if the work is done visibly and if it is performed in areas that fraud perpetrators may be considering. Fraud investigations that are done well put an unavoidable and often intolerable risk into the practice of perpetrating fraud. Most (if not all) fraudsters do not want to be caught. In those cases in which an entity fails to practice routine proactive checks, would-be fraud perpetrators are assured that, if they are careful and plan their fraudulent acts well, they run a minimal risk of discovery. However, if fraud avoidance efforts-particularly proactive auditing efforts—are expended periodically across a wide spectrum of an entity's operations, regardless of the purpose of the searches or their success in detecting fraud indicia, would-be and actual perpetrators will be on notice that any perpetration in those areas runs the risk of detection. Where there is little or no risk, only moral restraints keep people with few or no moral values from the easy money. Even though routine fraud examination may fail to detect any evidence of fraud, practice proactive investigation anyway. The risk of detection it imposes just may deter a would-be perpetrator.

Most investigators are basically nice people who feel comfortable with the impersonal aspects of their work. When describing incidents of waste, for example, most internal audit reports fail to mention who was responsible for the waste being reported. Fraud auditing is similar to, but different from traditional auditing in several ways. Typically, an audit starts with an audit plan, whereby, risks are identified through a risk assessment, controls are linked to the risks, sampling plans and audit procedures are developed to address the risk(s) identified. The audit steps are the same regardless of the

system(s) being targeted. Throughout the process, the auditor must have an understanding of the system(s) being audited. For example, to audit financial statements, auditors must understand generally accepted accounting principles (GAAP). In the same way, to audit a computer system, auditors must understand information technology (IT) concepts.

In the rapid pace of our changing world, it is difficult to keep up-to-date with industry trends in complex fields, such as data mining, text processing, crime mapping, link analysis, and other forms of advanced analytics. Many investigators are not adequately trained in the IT field-although this is changing as more advanced training is being provided to investigators coming up through the ranks. To better foster cooperation and data sharing among different agencies, and to alleviate the current non-collaborative investigative situation, fusion centers and programs have been proposed, are under development, or are actively operating to address these issues.

The main benefit of audit software is that it increases the ability of auditors and fraud investigators to probe the data, turning facts and figures into vital information. Audit software also makes extracting information from several files with different database management systems quick and efficient. Combining information from different sources can highlight relationships in the data. For example, reviewing data from an accounts payable file may identify a trend in the expenditures to a particular vendor. But combining the accounts payable data with information from the contracting database may reveal that all contracts with the vendor in question were raised by one contracting officer. This may prompt concerns about possible kickbacks.

Through a fraud scheme or "identified fraud risk," a fraud is perpetrated and concealed in a business system such as: account balance, class of transactions, or presentation and disclosure assertions. The fundamental mechanics of fraud schemes are the same for each organization, but how a scheme occurs within each organization may differ. Due to the differences, the identified fraud risks should be considered as an inherent risk. The search for fraud is built on both awareness and methodology; however, both items are predicated on auditors having a sufficient knowledge of the science of fraud, hence the fraud theory. Auditors are not born understanding fraud. The awareness needs to be incorporated into the audit plan through audit team discussions during the planning stages. Audit programs must incorporate a methodology that responds to the identified fraud risks existing in core business systems.

Concept of preventing unscrupulous staffs

As a result of fraud-related collapses, governments around the world have undertaken regulatory initiatives in the fraud area. These include rules under the Sarbanes-Oxley Act in the US and the Corporate Law Economic Reform Program in Australia. A fraud risk management framework is an essential element in meeting these corporate responsibilities of transparency and accountability. Developing such a framework is a complex task that requires an understanding of preventive standard for fraud and corruption control. An organisation must ensure this risk management framework effectively minimises fraud risk across all its operations, while at the same time having the flexibility to adapt to change. In order to capture fraud risk information from all staff, an electronic survey tool should be considered. This can be used across the organisation, or at the business unit or product-specific level.

Though laborious due to the gigantic volume of dynamic data available today, a full-view of customers and their activities is essential to monitor frauds and reduce the "false positives" effectively to an acceptable level. Control fraud occurs when a trusted person in a high position of responsibility in a company, corporation, or state subverts the organization and engages in extensive fraud for personal gain. The term "control fraud" was coined by William K. Black to refer both to the acts of fraud and to the individuals who commit them. The concept of control fraud is based on the observation that the CEO of a company is uniquely placed to remove the checks and balances on fraud within a company such as through the use of selective hiring and firing. These tactics can position the executive in a way that allows him or her to engage in accountancy fraud and embezzle money, hide shortfalls or otherwise defraud investors, shareholders, or the public at large. A control fraud will often obtain "investments that have no readily ascertainable market value", and then shop for appraisers that will assign unrealistically high values and auditing firms that will bless the fraudulent accounting statements.

Information technology is a significant part of the day-to-day operations for most organisations. But while the integration of technology results in many benefits, it also brings increased risks. Information technology fraud can be defined as a criminal act in which a computer is essential to the perpetration of the crime. It can include hacking, mail-bombing, spamming, domain name hijacking, server takeovers, denial of service, internet money laundering, destruction or theft of data, electronic eavesdropping and unauthorised transfers of funds, electronic vandalism and terrorism, and sales and investment fraud. It can also include a criminal act where a computer, not essential to the perpetration of the crime, acts as a store of information concerning the crime. Of course, entities generally face different fraud control issues depending on their size and the nature of their business, both of which influence an entity's potential exposure to fraud. It is not always practical to institute measures to address every possible business risk, including potential fraud. Therefore, it is important to carefully assess the likely occurrence of fraud and its impact on an entity's key organisational objectives and core business. A risk based approach enables an entity to target its resources, both in prevention and detection, at problem areas.

Furthermore, it is important to avoid looking at fraud in isolation from the general business of the entity. Entities are strongly encouraged to develop dynamic fraud risk assessment procedures integrated within an overall general business risk approach rather than in a separate program. However, some entities or programs will have an inherent risk of fraud due to the nature of their business. Those entities are encouraged to consider developing a fraud risk assessment process that is specific to a particular policy or program area, particularly when developing a new program or policy. Fraud control arrangements can reflect the fraud risk profile of an entity or particular program. While the nature and extent of fraud risks

faced by smaller entities may differ from the fraud risks facing larger entities, these risks will still require targeted mitigation strategies. Entities are encouraged to adopt fit-for-purpose mechanisms to address specific fraud risks. Additionally, fraud control plans can include review and oversight mechanisms to enable entities to evaluate the effectiveness of fraud control strategies regularly, particularly following changes in business processes or systems or after instances of fraud have been discovered. This will help ensure that control systems remain appropriate, cost-effective and proportionate to the actual risks they are addressing.

In short, the prevention and detection of fraud and impropriety is only possible where strong internal controls are present and constantly applied. Routine checks and monitoring by management to ensure that procedures are being followed are, therefore, essential. The benefits from implementing a culture of strong management controls are; a deterrent effect when it is known that management is actively involved in ensuring that procedures are followed; and the results of the checks will allow management to identify any operational areas where controls are not being uniformly applied and investigate whether systems have been exploited.

The continuing importance of forensic accounting

Today, fraud is more sophisticated - and devastating - than ever. In recent years, the complicated nature of modern fraud has driven the growth of forensic accounting, a niche field that is often referred to as investigator. Often trained in both accounting and criminal investigation, forensic accountants play a huge role in criminal justice and civil litigation.

Accountants may play a role in a dispute by acting as a mediator. For example, disputes involving business valuations, application of technical accounting standards or which require business acumen and experience in a particular industry or sector may benefit from having a mediator with the requisite expertise in these areas. In complex commercial disputes requiring an expert opinion on the quantum of damages, for example in a case whereby one party may have suffered a loss of profits following a breach of contract by another party, a forensic accountant may be retained as an independent expert to provide an independent assessment of the amount in dispute. In such a case the forensic accountant may be requested to prepare an expert report, attend a meeting of experts with an opposing expert, or advise their client on a range of their potential losses depending on a number of factors or assumptions. In mediation, the forensic accountant can provide a similar role, assisting a mediator in dealing with and understanding complex financial issues.

Many of today's financial disputes require specialized attention that even knowledgeable attorneys are unable to provide. Forensic accountants can lend a hand by deciphering complicated financial issues and relaying them in a way that both attorneys and their clients can understand. Forensic accountants may also play an investigative role in civil cases, working with attorneys to find unreported income or assets. In Mediation, a forensic accountant may be appointed in the role of a third party as a "data provider"; as someone who is "independent, neutral and impartial in their relationship to the parties, issues in dispute, and the data they provide". The forensic accountant may also have a role as a "data arbiter", i.e. an expert that may be retained by one or more disputing parties to answer factual questions about which the parties disagree and that they believe will be relevant to resolving the dispute.

With a complex, big data matter, there are generally very large quantities of information that need to be gathered and analysed. To be successful, this requires hiring expert teams and using the right tools to extract the critical information in a timely manner. Forensic accountants' investigative abilities can be put to good use, not only in standard civil disputes, but also in larger government investigations. For example, in major criminal investigations, forensic accountants can play a chief role in tracing complex money trails. Thus, they should be included in your organization's response team, working together with company insiders, counsel, and other professionals to maintain control of the investigation for your organization. Forensic accountants can perform an initial assessment of the situation and help the organization identify risk areas or gauge exposure for the organization. The organization may then undertake an initial assessment to develop a response plan to the investigation. This may include identifying individuals familiar with the underlying facts, determining supporting information that must be shared in the investigation, and formulating defence strategies.

Forensic analysis of data refers to analysis of electronically stored data. The most commonly analysed data are accounting and financial, but several non-financial categories of data are also very useful to investigators. Forensic accounting requires specialized knowledge and expertise beyond traditional accounting and audit skills. As such, forensic accounting professionals are trained to look beyond the numbers and leverage their understanding of accounting and auditing standards, business information and financial reporting systems, economic theories, data management, electronic discovery, data analytics, and litigation processes and procedures in order to complete their investigation and present their findings. The importance and need for a forensic accountant has become necessary due to failure in the routine audits, the intense economic pressures with companies facing bankruptcies and employees losing jobs, all these in turn giving way for frauds by the employees or even employers.

Reference

1. Bhatt GD. Knowledge management in organisations: examining the interaction between technologies techniques and people, Journal of Knowledge Management. 2001; 5(1):68-75.
2. Bressler L. Forensic Investigation: The Importance of Accounting Information Systems. International Journal of Business, Accounting, & Finance. 2011; 5(1):67-77.
3. Marcella Jr. Encryption Essentials. Internal Auditor. 2014; 71(6):55-59.
4. Wilkinson JW. Cerullo MJ, Raval B. Wong-On-Wing. Accounting Information Systems: Essential Concepts and Applications, New York:John Wiley and Sons, 2000.