The usage of technology in preventing and detecting fraud

Vjollca Karapici Ibrahimi

(Faculty of Economics, University of Tirana, Tirana, Albania)

Abstract: Auditors of information systems technology (IT) play a major role in the prevention of significant fraud and investigation. Fraud is hard to detect and even more difficult to prevent. All the auditors are responsible for detection, determination of fraud and use of anti-fraud programs. With rapid developments in information, communication and technology, it is no surprise that companies grow and secure IT system, but with the development of technology was developed and fraud schemes. Detection or not the auditor of the fraud, not fulfilling his work reflects you, or not drafting of a plan audit standards and procedures, but he has to do with personal ability auditor, to analyze the findings during the audit, use of tests, the natural limitations of internal control and the fact that most of the findings of the auditor of nature are more persuasive than effective. When you conduct an audit, auditor has a professional skeptic attitude that considers the risk of circumvention of control procedures by management and recognizes that simple fact, the audit procedures that are effective in connection with the discovery of errors, are not suitable for detection and identification fraud. This requires from the auditor to establish a procedure for considering the risk of fraud, in order to detect the exact appearance not as a result of fraud. A particular impact has The Model of Fraud Detection Strategy, as an 8 steps model for identifying fraud, using IT to collect, define and analyze the data and anomalies that highlight indicators of fraud.

Key words: fraud; technology; skeptic attitude

1. Control and audit of IT (information technology)

There is no doubt that the use of IT is changing the business' development within an organization in general and the nature of each function within the organization in particular. And as such, there is no doubt that the use of IT is changing the nature of the functions of audit, internal audit in particular. Exactly, without a support and deep technological knowledge, it can be very challenging and hard for the auditor to give their opinions.

Users of financial statements, in general, believe that one of the main objectives of the audits, especially IT, is the discovery of fraud. Auditors' responsibilities regarding fraud in financial statements begin with skeptical and professional attitude. Auditor neither assumes that management is not honest, nor assumes no questionable integrity. In exercising professional skepticism, the auditor should not be satisfied with less convincing evidences for the belief that management is honest.

Auditors of financial statements should know enough regarding fraud, noted its signs and signals, and should understand fraud and its potential situations. They require complex investigations, dealing with different fields of knowledge, as the financial economy, law and business practices, using traditional methods for detecting fraud. Fraud often consists of many cases or incidents involving repeated violations using the same method. Fraud cases

Vjollca Karapici Ibrahimi, Ph.D., associate professor, Faculty of Economics, University of Tirana; research fields: accounting and finance financial analysis and auditing.

that there may be similar in content and appearance, but usually are not identical (Palshikar, 2002).

Under the SNA[1] there are several types of fraud. Fraud is an intentional action (the worst interpretations of the essential facts), in order to convince someone to believe in this fallacy. This definition includes all the ways that people realize in order to lie, cheat, steal and victimize other people. There are patterns for every fraud case, helping the auditors to discover fraud and unlawful action. Many of those committing fraud, believe that are far and can not be caught, or that the schemes that use is very original. In fact, all frauds have the same indicators that help the deceiver in his crime and its auditor to search simultaneously. These include poor management, unethical behavior history, confused documents and disregard of procedure. These models are being conducted whenever a fraud happens. Some models are less obvious than others, but are still present.

Management fraud is intentional deception made by management that harms investors and creditors through the unreal (false) presentation of financial statements. Auditors of this are the managers, classes of victims are investors and creditors, and instrument to achieve this is the financial statements (Elliot & Willinham, 1980). Fraud management is also called “rogue financial reporting”.

Fraudulent financial reporting is defined as intentional conduct or reckless, resulting in essential misleading financial statements. This means the appearance of unfair trick to amounts in FS, as well as information related to notes on the statements in order to deceive financial statement users.

Audit of fraud relates to operations and procedures to detect financial fraud, using the accounting records and information, analytical relationships and knowledge of performing fraud and concealment schemes. Fraud examination work combines the expertise of auditors and investigators of crime. Auditor to recognize fraud involves the recognition of many elements: human capital, organizational behavior, knowledge on common fraud schemes, evidences and their source, standards etc (Bologna & Linquist, 1995).

Independent auditors of financial statements and fraud investigators perform their work in different ways. In an environment where electronics is widely used, auditor should study and test general controls and application of computers, to be consistent with the company’s controls.

Computer fraud is any fraud, which includes electronic data processing in support of committing or fraudulent actions. All the auditors should have sufficient familiarity with computers, electronic transaction processing and the computers’ controls to be able to complete the audit of a simple system and work with information system auditor. While financial computers’ frauds vary from the simplest to the most complex one, they affect financial institutions with an alarming frenzy. Moreover, financial computers’ frauds are difficult to detect in the usual course of business.

Technology has influenced the audit profession, and in the audit performance (gathering of information, analysis and control), and knowledge required to lead to appropriate conclusions, the efficiency, integrity. As a result of the development of technological skills of auditors, IT was developed. An IT audit aims to identify risks that are important in relation to financial fraud and their access to the FS in the accounting records or actions, in order to be drafted procedures and controls to reduce this risk[2].

The role of IT, control and audit, are related to the integrity, the importance of information system (IS) and financial reporting organization, in order to anticipate and avoid failures in them. Infrastructure and commercial electronics are integrated in business throughout the globe and the need for IT control and audit has never been so

[1] ISA (International Standards on Auditing).
[2] SAS No. 47, Audit Risk and Materiality in Conducting an Audit (AICPA 1984, 02).

great as today.

Audit of IT is an integral part of the audit function, because it supports the auditor's opinion on the quality of information processed by information system. Some of the key elements of IT audit are: screening and verification of the organization in accordance with IT, the legal bond which might jeopardize or replace organization risk, application-oriented principles of audit risk, the use of computer techniques and audit, application of standards such as ISO 9000/3 and ISO 17799 to improve the quality of the information system, etc.

2. IT auditor role in controlling and preventing fraud

All auditors are responsible for detecting, determining and using antifraud programs. Auditing standards[3] emphasize the auditors should exercise their professional skepticism to determine the risk posed by fraud. They require the auditors to assess fraud related to activity as a component of the internal audit function.

It is very difficult to prevent fraud which is considered under three main issues: prevention, detection, investigation. IT internal audit should help in preventing and detecting fraud. Some of the measures to be taken to prevent fraud are: Internal Audit (IA) must help to ensure the prevention of fraud by communicating information to the Internal Audit Committee and other related managerial committees; Insurance activity control of the IA should support the necessary confidentiality, anonymity, providing obvious evidence; Internal audit team can be instrumental in developing the risk profile of fraud within the organization and design audit programs to find areas of business thought to increase risk; IA can help to assess whether the tone and culture within a business is enough to recognize fraud as unacceptable behavior; Individuals must be receptive to the possibility of fraud and IA may play a role in auditing and efficiency of procedures for the detection and apprehension of fraud.

An element that helps in detecting fraud is a combination of internal audits work, internal control and external audits. However, there is a doubt that who discovers fraud, evaluates and tests the operating effectiveness of controls adopted. But in what percentage the cases of fraud are discovered by the auditor and especially by the IT auditor? Consequently, most of the IT audit programs appear to be focused on compliance with established procedures, standards of IT systems and internal control questionnaires (ICO), run in such a way to discover potential fraud and ensure the effectiveness of antifraud control. This is because there are gaps in the IT auditors such as: orientation towards technology or trends that have the IT auditors waiting fraud to be discovered by the financial auditor.

In completing the assessment of fraud risk associated with IT processes and controls, the IT auditor can build an ICO (internal control questionnaires) to evaluate and test the control, including antifraud program. While the financial auditor can evaluate the controls over financial data business, the IT auditor should focus on the area around the system ICT (information control technology) and processes related to ICT. IA helps growing the information over the existence and nature of the reporting structure, and handling reporting allegations. IA should see the trends and symptoms so that they focus attention on their future work and ensure the lessons of past fraud. The use of ICT in businesses nowadays includes evidence to be put on work in favorable way for verification and confirmation of an occurrence of fraud. Evidence collected by the ICT system can be used very well to find fraud case.

IT auditor tend to have the best team specializes in bringing IT systems, so they are able to detect fraud. IT audit begins investigations in many activities: as in terms of generation and recognition reports, identifying the

[3] (SAS) 99, AICPA (American Institute of Certified Public Accountants).

records and computer system, in terms of logical analysis of the computer system (analysis of the legality of the system etc).

Structured risk assessment of fraud, adjust the size of the organization, the complexity, industry and goals, should be performed and updated periodically. An organization should understand the risks of fraud and the specific risks that directly or indirectly applied to the organization to protect itself and its stakeholders in an effective and efficient fraud.

Assessment can be integrated with a general assessment of organizational risk, but should at a minimum level, include risk identification, risk assessment of the likelihood and importance of risk response. Assessment of risk of fraud by evaluating the likelihood and importance of fraud is related to IT processes.

The first industries that used techniques to analyze data to prevent fraud are phone companies, insurance companies and banks (Decker, 1998). An early example of successful implementation of the techniques of data analysis in the banking industry, is fraud in the Falcon system, which was based on a computer network (Brachman, et al., 1996).

Retail industries also suffer from POS fraud. Some supermarkets have begun to make use of digitized television closed-circuit (CCTV), together with details of POS transactions more susceptible to fraud (Ëeir, 2001).

Transactions of the internet recently have raised major concerns. Kerr (2002) suggests that fraud in transactions on the internet is 12 times higher than fraud in shops.

Fraud involving mobile phones, insurance claims, tax returns, transactions with credit cards, etc., pose significant problems for governments and businesses, but is not a simple task of fraud detection and prevention. Fraud is an adaptive crime, so it needs special methods of intelligent data analysis to detect and prevent it. These methods exist in the areas of Knowledge Discovery in Databases (KDD), the use of machinery and statistics. They successfully offer solutions and application in various areas of fraud.

3. Techniques for detecting fraud

The techniques used for detecting fraud that are divided into two main classes: statistical techniques and artificial intelligence (Palshikar, 2002). Examples of techniques of statistical data analysis are:

(1) Techniques of data processing for discovery, validation and error correction.

(2) Calculation of various statistical parameters such as averages, performance, probability distributions and so on.

(3) Probability distribution models of various business activity, or different terms or parameters of probability distributions.

(4) Classification of data to find patterns and between groups of data.

(5) Compatibility algorithms to detect anomalies in the behavior of transactions compared with patterns and known profiles.

Techniques are necessary to eliminate false alerts, risk assessment and predict the future of the current transaction. Management fraud is a knowledge intensive activity. The main techniques used for management of fraud include:

(1) Classification, aggregation and segmentation of data, so that these data can create interesting patterns, including those related to fraud.

(2) Expertise systems to detect fraud in the form of rules.

(3) Recognition of a model to detect similar classes, clusters, or patterns of suspicious behavior.

(4) Programming machines with techniques to automatically identify the characteristics of fraud.

(5) Networks that can learn suspicious patterns from examples and later used to detect them.

The analytical audit refers to technology analysis designed for the purpose of auditing and fraud detection. According to an analytical study of the ACFE[4], it was discovered that 46% of detected frauds occurred because of inadequate controls, 40% has used situations where controls are ignored and the difference is related to organizational elements. The primary reason why the audit analysis is used to detect the fraud is that a large part of the internal control systems have control's weaknesses. To effectively test and monitor internal controls, organizations should look at all transactions, to dig through them and to test these transactions compared with parameters determined through application, through systems and data sources.

A large part of the internal control systems can not handle this. Since many of these systems of internal control have some weaknesses, which can not be avoided, then all must be controlled to 100% of transactions. It is necessary to compare data from different applications and systems, and to be careful to not having crash, looking for double transactions, which are indicators of fraudulent activity or perhaps just lack of efficacy. High-risk areas should also be taken in consideration, so you can catch the fraud before it worsens the situation in the organization. What can we say about gathering samples (patterns)? While samples are needed for some processes, they may not be sufficient to complete testing of controls. Here are some of the elements that must be taken into consideration when determining the samples (patterns):

(1) The taking of samples is not fully able to quantify the impact and control failures, it is only able to estimate the errors within a population (sample) data.

(2) The taking of samples may miss very small anomalies, anomalies that may be aimed at vulnerabilities that can be used later causing a material breach (which may lead to fraud).

Fraud is not represented in a sample, so if you need to look for fraud, you must examine all transactions and do not use sampling.

Another key aspect of the audit analysis is the ability for technology of the IT to maintain and identify complete fraud, for all activities performed. If you find fraud, you will need proof of what you do to detect fraudulent activity. Tests should be specific and detailed enough to proceed to further investigation and even prosecution. This is why the certified Association Fraud Investigator, Institute of Internal Auditors and the American Institute of Certified Public Accountants, protect the theory of greater use of technologies, especially of IT, especially in analyzing data to help detection of fraud. But, which are some specific analytical techniques that can be used for detecting fraud? The following are some examples:

(1) Classification to find patterns and similarities between groups of data to identify trends and anomalies.

(2) The union or the compliance of data to identify employee's fraud and system failures.

(3) Chart to provide visual identification of abnormal transactions, such as journal entries manually whenever you have an unusual action.

(4) Identical copies of the test that identifies two models of simple or complex.

(5) Deficiency of testing, that identifies whether the missing bills or checks.

[4] ACFE, Association of Certified Fraud Examiner, USA (2008).

(6) Calculation of statistical parameters, such as averages, standard deviations and values higher and lower identifying statistical anomalies.

Audit analysis of more than 20 years is a proven and effective tool in combating fraud, and monitoring the effectiveness of internal controls to identify fraud risk. Traditional fraud detection usually begins with an anomaly or a sign that something is not right, such as stock tips, financial relations with unusual declaration or refusal of inspection.

These indicators, often called red flags (indications, signaling), make no doubt that fraud may exist. Managers, auditor, fraud investigators will investigate these indicators with additional research or interviews to determine if the red flags of fraud represent real or are caused by other factors. This approach can be viewed as an inductive method: It starts with anomalies and continues with research and additional information about events, until we discovered that fraud may be caused by several indicators. This will be followed by an investigation to determine which the current nature of these anomalies is.

Technologies and wider current use of electronic data in transactions have made it possible to identify specifically, various types of fraud, by examining the entire population (sample), and to naughting (become zero), before the fraud traditional indicators place so extraordinary as to be studied. This method is called strategic method of fraud detection. This method is a proactive approach aimed at achieving the objectives of the industry or company, and the identification of specific anomalies to detect fraud.

4. The strategic fraud detection model

Detection of fraud traditionally is performed by a pattern of fraud detection strategy of eight steps. Fraud investigators usually do not have any specific ideas in mind for fraud, but they see or point out an event or anomaly, which offers question and make inquiries.

(1) The strategic process begins with an understanding of business activity or unit to be controlled. To understand the business model is step one. Since every business environment is different even within the same industry or firm, the discovery of fraud is largely analytic process. Same procedures for detecting fraud can not be applied equally to all businesses or even in different units of the same organization. Rather than relying on the general methods for detecting fraud or specific actions, investigators must gain knowledge of specific details about each organization and its processes. Having a detailed strategic understanding, they can describe the entire process of detection of fraud.

(2) Once fraud investigators feel confident that they understand the business, they need to determine what possible fraud may exist or may occur during operation of the examination. Identification of possible fraud that may exist is the second step of the model of fraud detection strategy. This step for risk assessment requires an understanding of the nature of different tricks, as they occur, and what symptoms show.

Fraud identification process begins by conceptually separating the business in unit/individual department. Most businesses or entities are simply under too big and diverse to be considered simultaneously by investigators. The separation of business functions/departments of its individual focus helps in the process of discovery. For instance, investigators may choose to focus directly on the plant, sales department or the purchasing department. In this step, people involved in business functions have to be interviewed. Investigators fraud have questions such as:

a. What types of employees, vendors or contractors are involved? Who are the actors?

b. How to interact with other factors internal and external?

c. What types of fraud can be carried out against the company or on behalf of the company?

d. What can only workers or management, perform the trick?

e. How do you interact with consumers by sellers or alone, to commit fraud?

f. How do you interact with vendors or customers, to perform the trick?

Detecting fraud team during this phase must assume ideas of the kind of potential fraud and various players. Occurrence of various possible frauds and also a list of frauds that would be considered developed should be taken into account.

(3) The catalog of possible symptoms of fraud for each type of fraud is the third step of the model. Fraud is a crime that is rarely seen. Symptoms were observed only in the fraud. Unfortunately, it often seems to be a sign of deception, ends up being explained by other factors that are non-fraud. E.g., balance of accounts receivable in a company, can be grown at a high rate that seems unrealistic. But while this increase may be the result of fraud, growing balance of income may be the result of customers who have financial difficulties or a change in payment terms of credit.

This strategic approach must carefully be checked after taking into account the variation of six types of symptoms that may be present in the catalog of fraud identified in step 2. A matrix, tree diagram, or map of ideas can be created in correlation with specific symptoms of specific fraud.

(4) Once defined symptoms related to specific fraud and supporting data that are derived from corporate records and other sources, begins work on the use of technology to collect data on symptoms representing the 4th step. For this step of databases, data can be extracted in a similar way by different countries to preserve them. While traditional procedures and fraud detection require sampling data set, fraud detection technology must be run against a full part of the transaction. Any review or taking of samples, data is made, before the rights are enforced, restricts the power of the intelligence process, because the most important fraud can occur in very few transactions. In performing this step, fraud investigators should be prepared for bureaucracy and rules that make it difficult to gain direct access to databases. Access critical data directly is limited to users in many organizations. Such restrictions, intended to prevent multiple users to corrupt data, or viewing the information which should not have access.

Fraud investigators must have access to all data, to analyze information in a given system. Permission and support of senior management to have access to important information is very important to the successful efforts of fraud detection. Fraud detection teams should include a member of IT staff or IT audit, who understand the system and can provide access to it. To design and implement the symptoms effectively, an IT expert should be part of the fraud detection team. This person must be qualified on two areas: programming the database and the principles of fraud.

Programming skills in database is the main reason for that person to engage in the discovery team. He or she must have access to the database, and to understand the relationship between data. In addition, this person must have some ability to understand the principles of fraud, to contribute effectively to the discovery of the fraud team. IT experts can identify new symptoms of fraud, while they have an extract and analyzed data from previous questions.

(5) Once the relevant data are taken, they should be compared with the prospects and patterns. Analyzing and defining results is 5-step model of fraud detection strategy. Most of the data are analyzed frequently, so software must be written to perform automated analysis. These algorithms examine the data and highlight anomalies, the values of unknown suggested trends or issues that can be analyzed directly by investigators.

These special tests are unique to the business to be considered, and the type of fraud for which is being controlled. More detailed research includes time series models. This is because fraud is often detected, having reviewed the changes occur over time, such as and significant increase in costs or unexpected purchases are often a signal for possible fraud.

(6) Once abnormalities first noted and are determined to constitute an indication of fraud, they will be investigated using either traditional or technology based on the estimate. 6-step model of the fraud detection strategy will continue the investigation of symptoms. The investigation should be done only on anomaly that can not be explained through the continuous analysis procedures. Many times traditional investigations symptoms give us new insights that allow the computation of algorithms. Information about an anomaly often explains other significant findings recorded. These serve to “clean” computer methods, and provide more meaningful results.

(7) Investigators of fraud must follow all of the identified symptoms. Follow and repeat the cycle is to step 7 (optional), the model of fraud detection strategy. While, the finding of fraud is certainly the primary objective of efforts, often drawn out process to control weaknesses, effective systems, undocumented policies and data errors. Each of these anomalies can be corrected by making the company be more efficient and effective activities. Following, it has to not only eliminate the control weaknesses and fixing the system, but also include ways to discourage future acts of fraud (Albrecht, 2003).

Fraud detection process described so far provides valuable information that helps investigators, auditor and managers better understand the business and the types of fraud that may occur. Once the cycle is complete, the discovery team to explore what it has learned, and determine how we can improve. And with new tools and a set of algorithms tested, strategic deception detection process can begin again. Each iteration through the process should be more efficient and effective, than the first. The ultimate result is a more mature process and tested for the detection of fraud and other irregularities.

(8) Model of fraud detection strategy ends at step 8 (optional): automatic detection procedure. Since a large part of the discovery process is computerized, subsequent decisions are usually faster, because the analysis, algorithms and models, are already scheduled. As the tests become more refined, they can be integrated directly into business processes. They can be programmed into the new systems to prevent problems during data entry or transaction. They can be used to prevent abnormalities before occurring. In addition, defining measures in the form of procedures can be automatically periods. Procedures can be programmed to highlight the errors and send the results to security personnel.

5. Conclusions

Computer world is changing. Business operations are also changing, sometimes very quickly, due to the rapid improvement of continuous IT technology. Also, IT controls and audits are important. Today, people do their shopping from home via the networks. People use “numbers” or accounts to buy what they want through the computerized trading. So businesses are rapidly improving the technology and IT. Control, IT audit and security is a matter of everyone.

For the IT auditor, the need for auditing, security and control will be critical in the IT field and will be the challenge of this millennium. There are many challenges ahead, so all must work together to design, implementation and advocacy of the integration of these technologies in the workplace. The IT auditor should be

included in the audit, directly and indirectly. They should be informed about the impact of risk of fraud. There is no hesitation that the use of IT is changing the nature of the functions of audit, especially, internal audit.

Auditor of financial statements should know enough regarding fraud, noted for its signs and signals. They should understand fraud and its potential situations, adding his attention to preventing and controlling especially in some areas of IT controls through audit, including:

(1) Integration of control in the early stages of IT development projects.

(2) BIC increases the mandatory identification and EWS, as reference to estimate the fraud.

(3) Departure and parting in investigation of fraud through the identification detection and gathering directly to essential evidence.

(4) The ability to investigate and determine a trick by the IT auditor. This is significantly influenced by the auditor's knowledge of IT on business operations, processes and IT knowledge in the technical side.

References:

ACFE. (2007). *Report to the nation on occupational, fraud and abuse*. (Inter Business Issues, August)

Albrecht, W. S. & Willingham, J. J.. (1993). *The auditor's responsibility to detect and report errors and irregularities.* Evaluation of SAS No. 53.

Albrecht, W. S., Wernz, G. W. & Williams, T. L.. (1995). *Fraud: Bringing light to the dark side of business.* New York: Irwin Professional Publishing, 56-59,118-119.

American Institute of Certified Public Accountants (AICPA). (1993). *The expectation gap standards: Progress, implementation issues, research opportunities*. New York: Amer Inst of Certified Public.

Association of Fraud Examiners. (2007). *Fraud examiners manual*. Association of Certified Fraud Examiners, Inc.

Bologna, G. J. & Linquist, R. J.. (1995). *Fraud auditing and forensic accounting.* New York: John Wiley & Sons.

Dominique, G.. (2009, July/August). *Fraud—IT internal audit can make a difference.*

Elliot, R. K. & Willinham, J. J.. (1980). *Management fraud: Detection and deterrence*. New York: Terocelli Books, Inc., 4.

IT Governance Institute. (2007). *COBIT 4.1*.

KPMG. (2004). *Managing the business risk of fraud: A practical guide*. Retrieved from http://en.wikipedia.org/wiki/Data_Analysis _Techniques_for_Fraud_Detection.

The Auditing Standards Board. (2002). *Consideration of fraud in a financial statement audit.* SAS 99, American Institute of Certified Public Accountants.

(Edited by Ruby and Chris)