Research Journal of Finance and Accounting
ISSN 2222-1697 (Paper) ISSN 2222-2847 (Online)
Vol.6, No.14, 2015

Fraud Prevention and Detection

Dr. Shewangu Dzomira
Number 486 Greenfield Street, Masvingo, Zimbabwe

Abstract
Fraud has been a million-dollar business which is rapidly increasing at global level. Most organisations are victims of fraud which is committed in unlimited multifarious forms. Major threats have been prompted by new information systems, reengineering and reorganisation which weaken the existing controls. The paper addresses the anti-fraud strategy and fraud prevention and detection techniques.
Keywords: fraud prevention; fraud detection; anti-fraud strategy; perp-walk

1. INTRODUCTION

Fraud prevalence and adverse consequences associated with it, poses an argument that companies have to invest more resources and time towards fraud handling. It is the discretion of the company to commit these resources on fraud prevention or detection. Some business entities have significantly lower levels of assets misappropriation and less vulnerable to fraud reporting than other companies simply because they take proactive steps to prevent or detect fraud. Only those organisations which consider seriously fraud risks and take proactive measures to create the right climate condition to mitigate fraud occurrence have success in fraud prevention.

Of late, it should not surprise most executives or business leaders that a heightened consciousness of fraud and its prevention is serious to the success of any organisation. Culture compliance is the inception of the new and enhanced corporate governance requirements implementation. Despite the size of the organisation whether small or large, new or old fraud can just invade, therefore a check list mentality is not adequate and no matter how many internal control mechanisms are in place.

Prevention of fraud nowadays is not just a good business practice but should be a requirement. Most companies face several risks, each of which is huge and potentially destructive. The issue of vicarious liability stands out among these risks. Criminal acts committed because of organisational policy have held corporate and other entities liable for such acts. Employee criminal acts which are committed in the course and scope of their employment for the benefit of the business entity also make the corporation liable. Sometimes an employee can perform an unauthorised act on behalf of the organisation which held the organisation liable.

An organisation can institute a formidable fraud prevention program through financial risks from fraud losses, shareholders' lawsuits, prosecution, fines, and convictions for fraud. Emotional toll of fraud and reputational risk should be taken into consideration. The impact on the employees and families who have nothing to do with the company's fraudulent activities set the emotional toll since they suffer the consequences. For instance Enron employees suffered the personal devastation after being deceived like all other stakeholders who believed in the company. The employees in general saw their life savings, jobs and retirement plans disappear, as a result of corporate fraud and lack of executive integrity.

The assignment covers the concept of fraud prevention including fraud prevention techniques and fraud detection aspects and its tools and techniques of fraud detection.

2. FRAUD PREVENTION

Basing on other discussions on why people commit fraud, it is quite necessary for an organisation to adopt effective ways of dealing with the problem of fraud which will reduce stimuli, opportunity restriction and lowers potential ability of the perpetrators to rationalise their actions. Removal of fraud temptation and opportunity reduction from would be fraudster is the aim in the case of deliberately committed fraud.

Fraud prevention and losses prevention is profitable and can help to ensure stability and going concern.

It seems many companies do not have formal fraud prevention approach. Once fraud has occurred it is not easy to recover such losses, as such it is quite advisable to prevent such losses from occurring and the old saying *"prevention is better than cure"*.

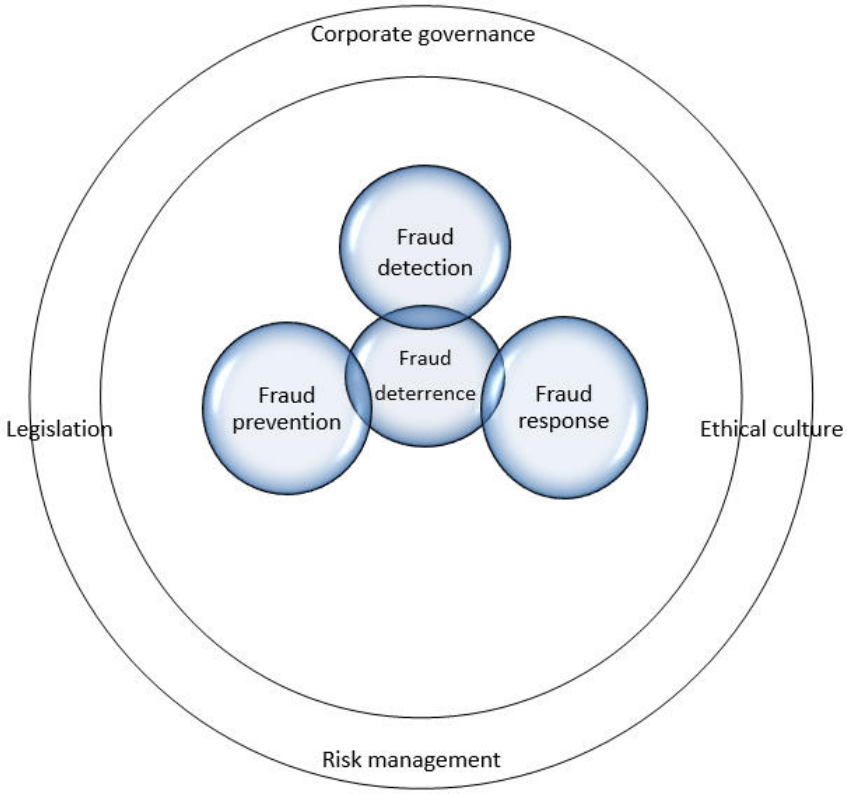
Prevention of fraud needs a system of policies and procedures which in their aggregate minimise the likelihood of fraudulent activities that may occur. The possibility of being caught mostly persuades the potential fraudsters not to commit fraud. As a result of this principle, the requirement of a thorough control system is necessary to fraud program. Any effective fraud program constitutes the critical aspects of "potential of being caught" and "the existence of a thorough control system". It is equally important to be proactive rather than reactive.

2.1 ANTI-RAUD STARTEGY

There are four main components which forms an effective anti-fraud strategy:

- Prevention
- Detection
- Deterrence
- Response

The summary of these elements is depicted by the following diagram and the context within which an anti-fraud strategy sits.



The elements of an effective and sound anti-fraud strategy from the figure above are closely related and each playing its essential role in combating fraud. Fraud detection can act as a deterrent by spreading a message to potential fraudsters that the company is fighting fraud and that necessary procedures are placed to pick any unlawful activity which could have happened. A potential fraudster would desist from committing the crime if there is a possibility of being caught. Sometimes prevention controls would be complimented by detection controls if they are insufficient. Suspected and detected fraud incidents need a consistent and comprehensive response, this will spread a message across that fraud is a critical issue and that subsequent action would be taken against the perpetrator. Any fraud case which is detected and investigated should strengthen deterrence and therefore, act as fraud prevention technique or measure.

2.2 FRAUD PREVENTION TECHNIQUES

2.2.1 DEVELOPING A SOUND ETHICAL CULTURE

A good foundation for a high and low risk of fraud environment is laid by the attitude within an organisation. Overlooking of minor unethical practices such as petty cash theft, and expenses frauds would mean that even the bigger frauds committed at higher management level might also be treated in the same lenient way. Of late, there may be a risk of complete collapsing of business entities either via a lone dangerous fraud or through a combination of several smaller frauds.

A trustworthy organisation is built from realisation by the suppliers, customers, employees and the community at large that the organisation stands on high ethical standards and it has taken time to consider their position on ethical issues. Also the afore-mentioned stakeholders would realise that dubious ethical or fraudulent activities would cause critical unfavourable consequences to the people and organisations concerned when exposed.

The following business principles would form the foundation/basis of a good statement of ethics:

- **Legal** – the organisation will operate within the law, licensing/authorisations obligations and any other regulations.

- **Risks** – assess and manage risk to our business operations.
- Communication – being truthful, accurate and helpful in communication.
- Assets – protect organisation's brand, intellectual, financial and physical assets.
- Information - protection of confidential company, employee and customer information.
- Competition – vigorous competing in market but in all fairness, trustworthy and honest in all dealings.
- Inducements – report and record any incident on gift acceptance or offers, hospitality, or any other inducements that lead or reward a decision, or engage in any way of bribery.
- Diversity – individuals are impartially and fairly treated, without prejudice and no harassment in any form.
- Environment – minimisation of hazardous effects of entity's activities on the environment.
- Healthy and safety – healthy and safety care on each other, our products and business operations.
- Conflicts – declare and avoid conflicts of interest that would lead to division of personal loyalties.

Committed CEOs or incidents which cause or almost caused organisational significant losses have created a positive ethical culture in some organisations.

Establishment of a sound ethical culture would need an organisation to have the following:

* Mission statement which defines how the organisation would want to be seen externally and refers to quality and to ethics.
* A channel of reporting suspected fraud.
* Management commitment through actions.
* An audit process which dwells on risk areas.
* Ethical and fraud reminding process for example annual letter and/or declarations.
* Limpid anti-fraud policy and business ethics statements, explaining acceptable and required behaviour in risk prone circumstances.

Anti-fraud and code of ethics policy in insufficient for fraud prevention, some ethical behaviour needs to be imbedded within organisational culture. **Higher level management commitment and "tone at the top"** is crucial. Most employees imitate the behaviour of superiors than to follow the ethics policy, so it is important that management should desist from applying double standards. To show commitment there should be adequate resources allocation to communicating ethics and values to employees, suppliers and business partners and where there is need to provide training.

In addition to senior management encouragement on setting ethical examples by their actions, corporate should ensure that the higher level management are committed to fraud risk controlling. A responsibility for fraud prevention should be assigned to show the employees that they are serious fraud and tackling would be considered at senior level. Policies and codes adherence should be closely and regularly monitored and policed by the appropriate persons of the organisation such as internal audit or senior management.

a) Periodic assessment of fraud risk

For fraud risk management, entities should periodically identify the risks of fraud within their organisations. All the fraud risk areas should be identified and business processes and then assessed in terms of likelihood and impact. Also the assessment should include apart from monetary effect, non-financial impact such as reputation.

Therefore, an effective fraud risk assessment would reveal the previously unidentified risks and reinforce the agility for timely fraud prevention and detection. Cost savings would be also identified as a result of fraud assessment.

b) Training and awareness of fraud risk

It is essential to conduct awareness via formal training and education programs as part of overall management of risk strategy. When major frauds occur most people who would be unwittingly close to it would be amazed and shocked that they were oblivion of what was transpiring. Specific concentration should be put on the managers and high risk areas operating staff, such as purchasing and expenses paying, and also those with fraud prevention and detection roles, for instance human resources and investigating staff.

Arguments on how far the fraud risk management training should stretch within an organisation beyond the audit team – for instance a common asked question is whether the staff and management who have been trained in fraud prevention measures would utilize the acquired knowledge in committing fraud. However, tip offs normally highlight fraud and it is equally important that all the staff is alerted of what entails fraud, fraud behaviour identification, and how to respond to fraud suspicion and fraud detection instances. As a result there is a benefit in covering fraud subject in generic terms, the corporate ethic, the audit approach and checks and balances built into processes. Such kind of training would decrease

rather than increase the number of fraudulent cases.

Employees can be educated via a number of media, such as formal training sessions, posters, group meetings, newsletters, payroll bulletins or awareness pages on internal websites. A combination of methods is normally most successful in ongoing communication. It is now pellucid that spending money on fraud prevention brings many benefits – while it is difficult to construct the cost benefit analysis. However, efficiency reduction and demotivated staff can be experienced as a result of excessive and expensive controls on fraud prevention.

c) Whistle blowing and mechanisms of reporting

One of the significant elements of fraud prevention programme is establishment of effective reporting mechanisms which can also have a favourable effect on fraud detection. People who are not involved in fraud usually know or suspect many frauds within an organisation. It is a big challenge to the management to persuade these "innocent" people to speak out – to demonstrate that it would be in their own interest. A whistleblower is influenced by the organisational culture on anti-fraud and reporting processes, as it is often fear of the results that has the impact. Trauma ranging from being dismissed to being shunned by fellow employees upon speaking out would be the impact to the whistleblower.

In cases where senior managers (as high as managing director), then the whistleblower's predicament is exacerbated. And this poses the management with greatest challenge – to convince the employees that it is everyone's responsibility to combat fraud and is good health to the organisation, and their future employment is potentially at risk from fraud.

Benefits of open whistle blowing culture include the following:

- Depicting of potential problems earlier.
- Deterrence of wrong doing.
- Critical information reaches the right people who can address the issue.
- Demonstration to stakeholders, regulators and courts that they are accountable and well managed.
- Reduces compensation and costs from accidents, investigations, litigation and regulatory inspections.
- Reputation maintenance and enhancement.

A good business sense is recognised by an enlightened organisation which implements whistle blowing arrangements.

Disclosure follow up is an essential element of any arrangement of whistle blowing. If employees know that something would be done after speaking out then they will speak up. In some cases the most common reason for not reporting a concern is thinking that it would not make a difference. The management should be alert of the risk of anonymous and malicious accusations, but they cannot throw away or ignore any report in case it would be correct. It is necessary for the management to include a clause in their policy that anonymous reports will be treated with extreme caution.

2.2.2 SOUND INTERNAL CONTROL SYSTEM

It could be considered that a strong internal control system is by a wide margin a most valuable fraud prevention technique.

a) Internal control responsibility

Organisational internal control system is the overall responsibility of the highest level in the organisation. Under the Companies Act, the directors are responsible for adequate accounting records maintenance. The Combined Code outlines that the board should maintain a sound system of internal control to safeguard the shareholders' investment and the company's assets. Taking into consideration the afore-mentioned from the Companies Act and Combined Code, the management should incorporate in their procedures designed to minimise fraud risk. It is the duty of the board to satisfy itself that the system is sound and gives a report to its shareholders on such review undertaken.

b) Internal control system

Policies and procedures taken together constitute an internal control system that supports an effective and efficient organisation's operations. Typically internal controls deal with factors such as processes authorisation and approval, controls on transactions and access restrictions, physical security and account reconciliations. Often these procedures include division of responsibilities and check and balances to reduce risk.

While segregation of duties is not always possible, the management should employ additional examination and control, which may include some form of internal audit as a regular feature. The nature and size of the organisation would determine the number and type of internal controls which an organisation can introduce. Fraud minimizing internal controls should where possible address fraud red flags.

In cases of new internal control procedures being introduced, they should be clearly documented in a simplified version, in order to identify any deviations. Regular reviewing of internal controls should be part of risk management process, and it is essential for continual improvement of controls in light of new risks, such as changing technologies and new markets, and innovative fraud perpetrators. Eventually, the internal control system should be embedded within the culture and organisation's operations.

c) Pre-employment screening

Pre-employment screening is a process of verifying potential candidate for employment's qualifications, suitability and experience. There are techniques which are used such as educational and professional qualifications confirmation, employment background verification and history on criminal cases. The organisation must get the person's written permission and all the documents must bear the potential candidate's name.

Applicants screening should reduce the possibility of individuals with dishonest and fraudulent behaviour being awarded a role within the organisation, and therefore it is a very important prevention of fraud measure. At a minimum, organisations should consider screening for cash handling posts, senior management positions and other trusted positions such as treasury and accounts payable. This screening process should not only be limited to new employees, but the checks should be run before any promotion and secondments into more senior or sensitive positions.

In case of agency employment process, organisations should never make an assumption on proper vetting of the potential candidate by the contracting agency.

2.2.3 PERP WALKS AS A FRAUD PREVENTION FORM

"Perp" or perpetrator walks have come to be expected in high-profile cases. It is the public parading of a high profile person charged with a serious crime before electronic media by law enforcement people, for the purpose of sending a strong message to other criminals that this can also happen to them. The public display of fraudsters sends a message and it serves as fraud prevention technique. A person is handcuffed from the streets up to the courts. The parading and plastering of the street walls, newspapers and television would send a clear message and deter potential perpetrators from committing the crime. The co-conspirators would also turn into informants and witnesses fearing to be perp-walked themselves.

The following is a 16 Step Fraud Prevention Plan that brings together the many of the elements described above.

i. Fraud risk consideration as an integral part of overall corporate risk-management strategy.
ii. Integrated strategy development for prevention of fraud and control.
iii. Ownership structure development from top to bottom of the organisation.
iv. Introduction of a fraud policy statement.
v. Introduction of ethics policy statement.
vi. Active promotion of these policies throughout the organisation.
vii. Control environment establishment.
viii. Sound operational control procedures establishment.
ix. Introduction of fraud education, training and awareness programme.
x. Fraud response plan introduction as an integral part of the organisation's contingency plan.
xi. Introduction of whistle blowing policy.
xii. Reporting hotline introduction.
xiii. Constant review of all anti-fraud policies and procedures.
xiv. Constant monitoring of adherence to controls and procedures.
xv. Establishment of learn from experience group.
xvi. Appropriate information and communication systems development.

3. FRAUD DETECTION

The bulk of the frauds are discovered accidentally or via information received, either by a tip off or by whistle blowing hotline. In most cases, greater losses are incurred as a result of employees ignoring the obvious. Finding and reporting of fraud and irregularities is the responsibility of everyone within the organisation, and it is equally important that an organisation has appropriate mechanisms of reporting.

Although external auditors do not necessarily detect fraud in many cases, but the internal auditors on the other side are most successful in serious frauds detection. Risk management procedures are more useful methods also to detect fraud. With permitting resources an organisation should form a strong internal audit team that would monitor and give advice on risk management issues and actively looking for fraud instances. It is not the responsibility of the external auditors to detect and prevent fraud, even though they should give reasonable assurance that the financial statements are free from misstatements (fraud and error).

Fraud can also be discovered through mechanisms and controls which would have been put basing on the advice from the internal and external auditors.

3.1 TOOLS AND TECHNIQUES

3.1.1 TOOLS

a) Training and experience

The training of management and staff (such as accountants, internal auditors) would form a good basis for anti-fraud implementation programme. Business processes understanding by accountants is very much crucial as is their expertise of the policies and procedures that should be in place within an organisation for efficient and effective operations.

b) Necessary mindset

Possibility of fraud within an organisation should not be written off; necessary mindset is needed that fraud is always possible. Professional scepticism should be maintained in potential fraud consideration. Sometimes it does not mean if someone works excessively on overtime, without going for leave, is in the process of committing a fraud or is covering up for fraud. However, necessary steps should be taken for further research.

3.1.2 TECHNIQUES

The techniques fall into two classes: statistical techniques and artificial intelligence;

a) Statistical data analysis techniques

- Time series analysis of time dependent data.
- User files computation.
- Pre-processing of data techniques for validation, detection, correction of error, detection and missing or incorrect data filling up.
- Various parameters of statistics calculation such as performance metrics averages and probability distributions.
- Probability distributions and models of various activities of the business.
- Finding patterns and associations among groups of data through clustering and classification.
- Algorithms matching for anomalies detection in transactions behaviour.

b) Artificial intelligence techniques

- Automatic identification of fraud characteristics by machine learning techniques.
- Encode expertise for fraud detection in rules form by expert systems.
- Neural networks that would learn patterns which are suspicious from samples.
- Recognition of pattern to detect classes, clusters or suspicious behavioural patterns approximately to match given inputs.
- Data mining to classify, cluster and data segmentation and automatic associations finding and rules in the data signifying interesting patterns, comprising those related to fraud.

4. CONCLUSION

Essential elements of an anti-fraud strategy would include a sound ethical culture and internal control system which is effective. The safeguarding of assets and financial risk exposure reduction can be attained through effective internal controls. However, not only a sound internal control system would provide total protection against fraudulent behaviour, but also other fraud prevention and fraud detection techniques.

Common fraud alerts are not useful unless there is fraud possibility acceptance. Incidence of fraud catastrophic is stopped by the awareness mindset within the organisation. The appreciation of the warning signs will make the signs more effective and such awareness can be attained by means of education and training continuing programme.

BIBLIOGRAPHY

ACL. (No date). Fraud Detection Using Data Analytics in the Banking Industry.

Alan D. Lasko & Associates, PC (2010 March/April). Detecting Fraud in Financial Statements.

Biegelman, Martin T. Bartow, Joel T. (2006). Executive Roadmap to Fraud Prevention and Internal Control: Creating a Culture of Compliance. Wiley.

Bolton, R. & Hand, D. (2002). Statistical Fraud Detection: A Review (With Discussion). Statistical Science

Bolton, R. & Hand, D. (2001). Unsupervised Profiling Methods for Fraud Detection. Credit Scoring and Credit Control VII.

Burge, P. & Shawe-Taylor, J. (2001). An Unsupervised Neural, Network Approach to Profiling the Behaviour of Mobile Phone, Users for Use in Fraud Detection. Journal of Parallel and Distributed Computing

Chin-Chen Lee. (2013, March).Detect Fraud before Catastrophe.

CIMA. (2009, January). Fraud Risk Management A guide to good practice.

Conan C. Albrecht. (No Date). Fraud and Forensic Accounting In Digital Environment. White Paper
Cortes, C. & Pregibon, D. (2001). Signature-Based Methods for Data Streams. Data Mining and Knowledge Discovery 5
Cox, K., Eick, S. & Wills, G. (1997). Visual Data Mining: Recognising Telephone Calling Fraud. Data Mining and Knowledge Discovery
Delloitte. (2010). Procurement Fraud Investigative techniques to help mitigate risk. ACL Services Ltd.
Estevez, P., C. Held, and C. Perez (2006). Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. Expert Systems with Applications 31
Fawcett, T. (1997). AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 AAAI Workshop. Technical Report . AAAI Press.
Fraud Advisory Panel. (2011, April). Fraud Facts.
Golden, Thomas W, Steven L, Skalak, Clayton. (2006). A guide to Forensic Accounting. J. Wiley.
Graham, Lynford. (2008). Guidance for Private, Government, and Non-profit Entities. John Wiley.
G.K. Palshikar, The Hidden Truth – Frauds and Their Control: A Critical Application for Business Intelligence, Intelligent Enterprise
Green, B. & Choi, J. (1997). Assessing the Risk of Management Fraud through Neural Network Technology. Auditing 16(1)
Karen Kroll. (2012, Sept). Keeping the Company Safe: Preventing and Detecting Fraud.
Keller & Owens. (no date). Preventing and Detecting Fraud in Not-for-Profit Organisations. LLC
Michalski, R. S., I. Bratko, and M. Kubat (1998). Machine Learning and Data Mining – Methods and Applications. John Wiley & Sons Ltd.
Murad, U. & Pinkas, G. (1999). Unsupervised Profiling for Identifying Superimposed Fraud. Proceedings of PKDD'99.
Nigrini, Mark (June 2011). "Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations". Hoboken, NJ: John Wiley & Sons Inc.
Peter Millar. (2010 August 16). Seven Steps to Jump Start Your Anti-Fraud Program.
PWC. (2008 December). A practical guide to risk assessment.
PricewaterhouseCoopers LLP (2009). "2009 Global Economic Crime Survey". Retrieved June 29, 2011.
Phua, C., Lee, V., Smith-Miles, K. and Gayler, R. (2005). A Comprehensive Survey of Data Mining-based Fraud Detection Research. Clayton School of Information Technology, Monash University.
Thomas P. DiNapoli (no date). Red Flags for Fraud. State of New York Office of the State Comptroller.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar