Research Journal of Finance and Accounting
ISSN 2222-1697 (Paper) ISSN 2222-2847 (Online)
Vol.5, No.15, 2014

Fraud Risk Assessment: A Tool for SME's to Identify Effective Internal Controls

Geetha A Rubasundram
School of Accounting, Finance and Quantitative Studies, Asia Pacific University, Technology Park Malaysia
57000, Kuala Lumpur
Email : geetharubasundram@yahoo.com

Abstract
In recent years, the importance of good control mechanisms has increased significantly due to the number of high-profile corporate failures caused by top management fraudulent acts. Sarbanes Oxley Act 2002, Section 404 says that it is the management's responsibility to maintain and assess the effectiveness of its own internal control structure for financial reporting. The Act also states that it is the auditor's responsibility to attest and report on the management's assessment and the state of the overall financial control. Previous research that had been carried out was from the perspective catered mainly for the auditors or audit committees that had been set up by the management of the organization. Not many organizations, especially Small and Medium Sized Organizations are able to afford the cost of hiring consultants, auditors (external and internal) or set up audit committees to assess and manage the Internal Controls**.** Therefore, this paper expects to provide guidance to smaller sized organizations that prefer to set up and maintain effective and efficient Internal Controls in-house; on how to carry out a Fraud Risk Assessment and recommend Internal Controls based on the results, whilst trying to ensure costs, personnel and operations turnover are not affected in an unreasonable manner.
Keywords: Fraud Risk Assessment, Internal Controls, Fraud Schemes, Fraud, Small & Medium Sized, Community Manager

1.0. INTRODUCTION

After the collapse of Enron, WorldCom and other failures of high profile corporations due to fraudulent activities, many organizations, and stakeholders around the world have focused their efforts to minimize the risk of fraud within their organizations. Fraud has been defined as an intentional act designed to deceive others, resulting in the victim suffering a loss after relying on the deceit and the perpetrator achieving a gain (AICPA et al, 2008, p.5) This definition is agreed by The Institute of Internal Auditors, Association of Certified Fraud Examiners and The American Institute of Certified Public Accountants in their joint publication: Managing the Business Risk of Fraud: A Practical Guide. A more detailed discussion on the definition of fraud is available in the literature review section.

With the collapse of these companies due to fraudulent activities, the losses suffered were huge and affected many stakeholders such as:-

- Employees to have lost their jobs
- Shareholders to have lost their investments
- Suppliers who had provided services to the organizations to not receive their payments
- Banks who had loaned or advanced funds to lose their advances
- Customers who had paid for the services to lose their money
- Economy of countries to be affected

A survey done by PricewaterhouseCooper's in 2007 known as the Global Economic Crime Survey, (PWC, 2007, p.4) found that over 43% of the 5,428 companies from 40 countries that took part in their research project had suffered one or more significant economic crimes during the previous two years. The same survey on page 8 attempted to identify the cost of losses from fraud., Although the survey has managed to show that the estimated loss has increased from USD 1.7 Million on average per company in 2005 to USD 2.4 Million in 2007, it was mentioned that this figure could have been undervalued due to the inability of the executives interviewed to place a confirmed figure on the losses. The Association of Certified Fraud Examiners (ACFE, 2010, p.9) agrees with the above survey in the "Report To The Nations 2010", where it states "The inherently clandestine nature of fraud means that many cases will never be revealed, and of those that are, the full amount of losses might not be uncovered, quantified or reported. Consequently, any measurement of occupational fraud costs will be, at best, an estimate. In any event, it is undeniable that the overall cost of occupational fraud is immense, certainly costing organizations hundreds of billions or trillions of dollars each year". Hence, looking at the high cost of fraud, the need for organizations and business to focus on preventing, detecting, and responding to fraud is extremely high.

The Association of Certified Fraud Examiners– Report to the Nation 2010, (ACFE, 2010) mentions that fraud is likely to be detected by tips from whistleblowers (40.2%), management review (15.4%) and internal

audit (13.9%). Having anti-fraud controls appears to have helped reduce the cost and duration of fraud schemes. The report had looked at the effect of 15 common controls on the median loss and duration of the frauds. Victim organizations that had these controls in place had significantly lower losses and time-to-detection than those organizations without the controls.

THE RESEARCH PROBLEM

The writer of this paper could not find relevant literature written for an in house management team from Small and Medium Sized Organizations. Small and Medium Sized Enterprises are defined by the European Commission as having less than 250 persons employed. They should also have an annual turnover of up to EUR 50 million, or a balance sheet total of no more than EUR 43 million (European Commission Recommendation of 6 May 2003).

Therefore, the objective of this paper was to introduce and implement efficient and effective Internal Controls for the Small and Medium Sized Organisation. In larger organisations, the division of roles and responsibility may prevent fraudulent acts due to the necessity and risk of collaboration. However, in smaller sized firms, more often than not, the decision maker or authorised signatory may be limited to one person, or minimal persons. Hence, the risk of fraudulent acts occurring may be higher as compared to larger firms. The Association of Certified Fraud Examiners (1998) reported that organisations employing less than 100 employees were the most vulnerable to the risk of fraud. This is also discussed by Shanmugam et al (2012).

The selection of choice for the Case Study is a Community Manager using the recommended process identified during the literature review and the carrying out of the selected research methodology. A definition which the writer found very close in description to the actual role of the Community Manager is in Wikipedia. Although the writer is aware that Wikipedia is not an accepted source, but for the sake of providing a description of the term, it has been included here. As briefly defined by Wikipedia, a Community Manager is a manager of a "condominium or homeowners association including single-family home subdivisions, townhouses, or mixed-use development". A similar description is provided by Hyatt (1975, p. 979) where he discussed about the set up of a Homeowner Association in a condominium. He mentions that the owner is not only interested in the unit that he buys, but also the amenities, the grounds, the exterior of the building etc. Usually the Owner Association is either run by the owners themselves or they hire a manager or management company to manage it for them with periodic reporting. The role of the Community Manager is discussed and explored further in later sections of this research paper.

This study explores the gap between the methodology used by auditors (internal and external) as compared to an organizations internal management to provide a guide that is relevant and applicable to all small and medium sized organizations to carry out a Fraud Risk Assessment and Management, as well as identifying Internal Controls.

2.0. LITERATURE REVIEW

2.1. DEFINITION AND ELEMENTS OF FRAUD

Fraud has been defined as an intentional false representation by one party in order to gain unlawfully at the expense of another who relied on the false information provided. This is agreed by Ruin (2009, p.88), CIMA (2009, p.7) and Wells (2007, p.2). Examples of fraudulent activities include theft, corruption, bribery, embezzlement, money laundering, and others, which causes financial losses to a corporation (CIMA, 2009, p.7). A more corporate definition of fraud comes from the Statement on Auditing Standards 99 (SAS 99). SAS 99 defines fraud as an intentional act to cause a material misstatement in the financial reports, either by falsification of accounting records, misappropriation of company assets such as theft or fraudulent expenditure amongst others (Ruin, 2009, p.99). The Australian Auditing Standard ASA 240 (2006, Para. 9) agrees with the SAS 99 saying that it is an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.

The focus of this paper is on Corporate Fraud; therefore, the victim party with losses due to fraudulent activity is the Corporation itself. However, perpetrators of fraud may not necessarily be within the Corporation itself. O'Bell (2009) mentions that an individual within an organization or external to the organization can perpetrate fraud. For clarification purposes, organization and corporation signifies the same in this paper.

If the possible perpetrators were from within the organization such as the employees of the organization, then they would be committing Occupational Fraud. Wells (2007, P.1) defines Occupational Fraud as the misuse of one's occupation in order to achieve personal enrichment through the deliberate misuse or misapplication of the employing organizations resources or assets. Wells (2007) mentions the following points need to be present to proof a fraudulent activity occurred in the first Report to the Nation on Occupational Fraud and Abuse in 1996:

- Clandestine and violates the employees fiduciary duties to the organization
- Committed for the purpose of direct or indirect financial benefit to the employee

- Has costs the employing organizations losses in terms of assets, revenues, or reserves.

An employee's fiduciary duty involves acting in good faith and in an honest manner when being entrusted in handling assets or benefits of the assets not belonging to him, i.e. in a position of a trust (Wells, 2007, p.2). An example of a violation of Fiduciary Duty would be if a Purchasing Manager takes bribes from a supplier and awards the same supplier contracts regardless of their capabilities and experience.

There have been studies carried out to understand what makes persons in a position of trust, to become violators of the same trust given to them. Most of the current literature read is from the research carried out by Edwin H. Sutherland and Donald R Cressey (Wells, 2007, p.7). Sutherland was the first to define "white colour crime" in 1939 which meant criminal acts of corporations and individuals acting in their corporate capacity. Sutherland later developed the "theory of differential association" which was against the view then of "criminals beget criminal offspring" (Wells, 2007, p.7). Sutherland believed crime maybe learnt by communicating with others and should take into account environmental factors. A more recent literature is the research done by Donald R. Cressey, who was a student of Sutherland (Wells, 2007, p.8), a theory now popularly known as the Fraud Triangle.

2.2. FRAUD TRIANGLE – MOTIVE, OPPORTUNITY & RATIONALIZATION

Cressey's focus was on embezzlers and the circumstances that would cause the then employees to become trust violators. Wells, (2007, p.2) defines embezzlement as to intentionally misuse the benefit or use of an asset which has passed on to the embezzler via a position of trust or agency, for the benefit of the embezzler. Cressey interviewed about 200 convicted offenders during his research. Cressey's final conclusion was that trusted persons become trust violators when they view themselves as having a non-shareable financial problem that is solvable using unethical means by violating their position of trust. The trust violators believed that they had a right to use the organization's assets and benefits assigned to the assets. (Wells, 2007, p.6)

Over the years, Donald Cressey's hypothesis or popularly known as the Fraud Triangle where one leg of the triangle represents pressures or motivation to carry out the fraud, the other is the opportunity available to carry out the fraud and the final is rationalization.

CIMA (2009, p.13) mentions the same whereby:-

- Motivation or pressure is typically based on either greed or need
- Opportunity for fraud to take place is more likely in companies where there is a weak internal control system, poor security over company property, little fear of exposure and likelihood of detection, or unclear policies to concerning acceptable behavior.
- Rationalization of the fraudulent behavior by the perpetrators as necessary, harmless, or justified.

'O Bell, (2009) mentions that when all three of the above conditions (motivation or pressure, opportunity and rationalization) are present, the risk of fraud being perpetrated can increase significantly.SAS 99 agrees that motivation or pressure, opportunity and rationalization are three conditions that can increase the risk of fraudulent activities occurring in an organization. Any method identified to reduce the risk of fraud in an organization should focus on reducing the three conditions identified in the fraud triangle.

2.3. METHODS TO PREVENT & DETECT FRAUD

O'Bell (2009) mentions that of the three conditions (opportunity, rationalization, and motivation); opportunity is the one condition that is manageable to address fraud risks. This condition is managed by designing and implementing a control environment that prevents, detects, and deters most fraudulent behaviour, whether conducted by employees, vendors, consultants or senior management.

CIMA (2009, p.15) mentions that one of the most effective ways to tackle the problem of fraud is to adopt methods that will decrease the motive or opportunity, or preferably both. Rationalization is personal to the individual and more difficult to combat.

This paper followed 'O Bell's recommendation and focused on reducing Opportunity by implementing a control environment to prevent, detect and deter fraudulent behaviour and activities. Rationalization as agreed by both CIMA and 'O Bell is more personal and difficult to control. However, pressures and motive, although recommended by CIMA (2009, p.15), would not be part of the factors taken into consideration in this paper in agreement with Cressey. Cressey considers pressures or motive as a non-sharable problem by the perpetrator (Wells, 2007, p.6); hence, it may be a personal issue to the individual.

2.4. DEFINITION OF A CONTROL ENVIRONMENT AND INTERNAL CONTROL SYSTEM

O' Bells recommendations of implementing a control environment with strong internal controls to prevent, detect, and deter fraudulent behaviour is agreed by the Association of Certified Fraud Examiners (ACFE, 2010). Having sound internal controls systems is also a requirement under the Companies Act, Sarbanes Oxley, Turnbull Guidance, and various corporate governance codes. (CIMA, 2009, p.33)

A Control Environment, according to The Committee of Sponsoring Organizations of the Treadway Commission

(COSO), establishes the foundation for the Internal Control System by providing fundamental discipline and structure (Verschoor, 2008). COSO 1992 - 2004 defines Internal Control System as a process, implemented and managed by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives regarding:

(i) Company strategy;
(ii) Effectiveness and efficiency of operations;
(iii) Reliability of financial reporting
(iv) Laws and regulations compliance

Rikhardsson (2006, p 2&8) mentions factors that contribute to the control environment which include:

- Integrity
- Ethical values
- Competence of the entity's management and employees
- Management's philosophy and operating style
- Assignment of authority

Therefore, a sound ethical culture and an effective system of internal control are essential elements of an anti-fraud strategy. The Control Environment and Internal Control System should be an initiative by top management as agreed by Rikkhardsson, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) and CIMA,(2009, p.33) says that the overall responsibility for the organization's system of internal control must be at the highest level in the organization. The emphasis on management integrity is also discussed by Turner et al (2003), identifying the connection between incentives, opportunity and management integrity.

For the Control Environment and Internal Control System to be successful, the Internal Control System has to be included with the vision and mission of the company to achieve the companies' objectives in an effective and efficient manner. Internal controls operate on many levels. There could be behavioural controls, information controls, operational controls, preventive controls, detective controls, application controls, and general controls (Rikkhardsson). CIMA (2009) also provides examples of areas where Internal Controls typically exist such as approval and authorization processes, access restrictions and transaction controls, account reconciliations, and physical security. These procedures often include the division of responsibilities, checks and balances to reduce risk.

Setting the control procedures and policies should not be a one off exercise and should be reviewed continuously. When new policies are set in place, it should be done in a clear manner, documented and communicated to all within the organization (CIMA, 2009, p.34). Regular review of internal controls is part of the risk management process, and there should be continual improvement of controls taking into account of possible new risks, such as new markets and technologies, changes in structure, or innovative fraudsters. Ultimately, the internal control system should be part of the culture and operations of an organization (CIMA, 2009, p.34)

2.5. COST BENEFIT ANALYSIS OF INTERNAL CONTROLS

Nevertheless, too many controls could proof to be costly and time consuming, hence may cost the organization to lose more due to a bureaucratic environment. The same view is shared by CIMA (2009), whereby the Internal Control System consists of an organization's policies and procedures that when taken together, support an organization's effective and efficient operation.

Verschoor, (2008, p.141) mentions that management should evaluate the controls that have been implemented to ensure that the risk of a material misstatement in the financial statements could happen would be prevented or detected in a timely manner. The approach taken should be top-down and risk based, to ensure efficiency of operations by allowing management to focus on those controls that are needed to adequately address the risk of a material misstatement of its financial statements and does not require the organization to identify every control in a process or document the business processes impacting the organization (Verschoor, 2008, p.142).

2.6. RISK ASSESSMENT AND MANAGEMENT

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has outlined five essential components of an effective internal control system. Apart from the control environment, it also includes communication and monitoring of the policies and controls set in place (Verschoor, 2008). The remaining two components are:

- Risk Assessment, an analysis carried out by management to identify risks that could prevent the achievement of predetermined objectives
- Control Activities, which consists of the policies, procedures, and practices, that ensure management objectives and risk mitigation strategies are carried out and achieved.

O' Bell (2009) recommends carrying out a fraud risk assessment as part of the anti-fraud controls to be

implemented, which is in line with the recommendation from The Committee of Sponsoring Organizations of the Treadway Commission (COSO) excerpt above, except that it focuses on the risk of fraud purely. Since, this paper also covers Internal Controls that need to be set in place, it shall also take into account the five essential components from the Risk Management Strategies as mentioned in The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

CIMA (2009, p.17) defines Risk Management as the process of understanding and managing risks that the entity is inevitably subject to in attempting to achieve its corporate objectives (CIMA official terminology, 2005). One such risk is fraud risk, a component of operational risk. Operational risk focuses on the risk associated with errors or events in transaction processing or other business processes. A fraud risk review considers whether these errors or events could be the result of a deliberate act designed to benefit the perpetrator. The possible type of offence and the potential perpetrator classifies fraud categories and the risk from each area and process of the business is gauged (CIMA, 2009, p.21).

The risk management cycle is an interactive process of identifying risks, assessing their impact, and prioritizing actions to control and reduce risks. CIMA recommends the following steps (2009, p.19):

- Establish a risk management group and set goals.
- Identify risk areas
- Understand and assess the scale of risk in the initial stages itself.
- Develop a risk response strategy. Before developing the strategies, it is necessary to establish the risk appetite of the organization. Risk appetite is the level of risk that the organization is prepared to accept and this should be determined by the board. The appetite for risk will influence the strategies to manage risk (CIMA, 2009, p22).
- Strategies for responding to risk generally fall into one of the following categories :-
    - Risk Retention (e.g. choosing to accept small risks)
    - Risk Avoidance (e.g. stopping sale of certain products to avoid the risk of occurring)
    - Risk Reduction (e.g. through implementing controls and procedures)
    - Risk Transfer (e.g. contractual transfer of risk; transferring risks to insurers)
- Implement the strategy and allocate responsibilities. - Clear assignment of responsibility and target dates, including budgetary changes (CIMA, 2009, p.22).
- Implement and monitor the suggested controls - The chosen strategy may require the implementation of new controls or the modification of existing controls. Controls implemented need to be assessed together with the companies dynamic business objectives (CIMA, 2009, p.22).
- Review and refine the process continuously. (CIMA, 2009, p.22)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework , Vershoor (2008, P.131) and Rikhardsson(2006, p.19) agrees that just like the Internal Control Environment, the risk appetite is set by the entity's top management and will be used to influence the strategies set in order to achieve the objectives set by the entity. Verschoor, (2008, p.131) mentions that according to COSO, there are eight components of Enterprise Risk Management which in turn is similar to the risk management cycle recommended by CIMA.

This paper will be following the recommendation in this section to carry out the Fraud Risk Assessment and setting of an effective and efficient Internal Control Environment.

2.7. CARRYING OUT A FRAUD RISK ASSESSMENT

CIMA and The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recommend carrying out a Fraud Risk Assessment prior to implementing internal controls. This is to ensure proper focus, identification, and management of fraud risk in an organization. O' Bell (2009) believes that the Fraud Risk Assessment helps to focus management's attention on the significant fraud risks to be addressed and managed. An effective Fraud Risk Assessment may include:

- Specific fraud schemes that could be perpetrated against the organization
- The personnel or departments within the organization that could commit each scheme
- The likelihood of that scheme occurring against the company in the current year
- The magnitude of impact that the scheme would have on the organization
- Assessment of the existing internal controls to mitigate fraud, and the identifying of any gap required to update controls.

Beran (2009) also provides a guideline to carry out a Fraud Risk Assessment through conducting brainstorming sessions with management to discuss potential fraud schemes and scenarios. A Fraud Risk Matrix includes each process owner, possible fraudulent activities, and scenarios affecting the process, and a detailed account of all controls in place to prevent or detect fraudulent activity to be created to monitor and gauge. Once a Fraud Risk Matrix is developed, reviews can be performed or select processes to evaluate the effectiveness of the

stated controls to mitigate the fraud risks. The matrix provides the ability to perform a gap analysis to identify areas where anti-fraud control is required.

The North Dakota State Government guideline for carrying out a Fraud Risk Assessment agrees with the steps of setting up a risk assessment team and carry out a brainstorming activity and other methods such as interviews with other personnel to understand the organizations business process, gather information about potential fraud, identify the fraud risks, including the factors of the Fraud Triangle, risks of management override of controls, an understanding of the fraud risk and the subset of risks specific to the organization.

CIMA, (2009, p.20) agrees with the above and also mentions some of the techniques that can be used for analysis and identification of risk areas such as workshops, interviews, brainstorming, questionnaires, process mapping, and comparison with other organizations and discussion with peers. However, the resulting document is known as a Risk Register (CIMA, 2009, p.21), as compared to Beran's (2009) version of the Fraud Risk Matrix. The Risk Register and Risk Matrix are just different in name, but contents are the same, therefore both terms will appear and mean the same in this paper.

The below steps have been identified to carry out a successful Fraud Risk Assessment & Management:

1. Management to initiate the Fraud Risk Assessment & Management by setting up a Fraud Risk Assessment & Management Team (FRAM Team) to set goals, objectives and the fraud risk appetite of the organization.
2. FRAM Team to carry out brainstorming activities, process mapping, necessary checks, audits & tests and discussions / interviews with other personnel to understand the following:
    - 2.1 The organizations environment, management, business, departments, processes , functions and owners
    - 2.2 Potential fraud scenarios and schemes, taking into account red flag areas such as management override of controls and personnel who may have the three factors identified in the Fraud Triangle – Opportunity, Rationalization and Motivation
    - 2.3 Identify the categories required and assess the likelihood and impact of the fraud schemes accordingly
    - 2.4 Based on the above, do a review and gap analysis of the current controls in place and any additional or revised controls needed, in line with the organizations risk appetite and decided risk strategy
    - 2.5 Implement and monitor controls with periodic evaluation.

Based on Step 1, the Fraud Risk Assessment & Management Team preferably consists of individuals from different backgrounds, knowledge, skills, and perspectives. A suggested mix from North Dakota State Government is:

- Accounting / finance personnel who are familiar with the financial reporting process and internal controls
- Non financial business unit and operations personnel, to leverage their knowledge of day to day operations
- Legal and compliance personnel
- Internal Audit personnel

For Step 2.2, the North Dakota State Government guide mentions that each division or function needs to carry out a fraud assessment. Functions and services that need to be included in the assessment are Finance and Accounting, Human Resources Management (payroll), Purchasing and Contracting and Information Technology.

2.8. FRAUD TREE: CLASSIFYING CATEGORIES OF FRAUD

In order to list specific fraud schemes, this paper reverts to (Wells 2007, p. 44 – 45), where it states that it is better to classify and categorize occupational fraud, rather than lumping them into a general category, as by comparing schemes in well-defined categories, common methods used by the perpetrators and common vulnerabilities in the victim organization that allowed these frauds to succeed. This in turn should help in the development of better, more efficient anti fraud tools. After the Report to the Nation study in 1996, the Fraud Tree classification system was set up that accounted for most, if not all, of the most common occupational fraud and abuse schemes.

According to the Fraud Tree, there are three major categories of occupational fraud:

- Asset Misappropriations
- Corruption
- Fraudulent Statements

Wells (2007, p.51 – 52) defines Asset Misappropriation as the misuse of any company asset for personal gain. The book refers to Marshall and McManus definition of assets whereby "Assets are probable future economic benefits obtained or controlled by a particular entity as a result of past transactions or events. There are two broad definitions of assets, tangible and intangible. Intangible assets are difficult to misappropriate

because they are not physically identifiable. Hence for all practical purposes, asset misappropriations are restricted to tangible assets. Tangible assets for accounting purposes, are classified on the entity's books as one of five principal types, cash accounts receivable, inventory, plant and equipment, or investments.

The second category of occupational fraud is Corruption, which is defined as "an act done with intent to give some advantage inconsistent with official duty and the rights of others (Wells, 2007, p.278), which in turn can be broken down into Conflicts of interest, Bribery, Illegal Gratuities and Economic Extortion (Wells, 2007, p.281).

The third category is Fraudulent Statements where can be segregated into financial and non-financial. Wells mentioned that it would be easier to prevent and detect fraud by understanding the different pressures faced by senior managers to drive them to commit fraud such as to show a positive performance, or losses etc. (Wells, 2007, p.328).

Examples of fraudulent statement schemes are Fictitious Revenues, Timing Differences, Concealed Liabilities and Expenses, Liability / Expense Omissions, Capitalized Expenses, Improper Disclosures, Improper Asset Valuations etc. (Wells, 2007, p. 361)

The same categories are mentioned by CIMA (2009, p.8) and the North Dakota State Government. The actual specifics and breakdowns of the categories, and the departments or personnel involved will not be covered here, even though it was read as part of the Literature as instead, it will be directly covered under the Fraud Risk Matrix towards the end of this paper.

2.9. ASSESSING THE LIKELIHOOD AND IMPACT OF THE RISK OF FRAUD

The next step after identifying possible fraud scenarios is to assess the likelihood and impact of the risk of fraud. The North Dakota State Government article suggests assessing the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes and interviews with staff, including business process owners.

The North Dakota State Government guide recommends the following to assess both the likelihood and impact as follows:

- Likelihood: To assess based on the instances of that particular fraud occurring in the past in that organization, the prevalence of the fraud risk in industry and other factors, such as the number of individual transactions, the complexity of the risk and the number of people involved in reviewing or approving the process. Recommended categories to adequately grade the likelihood is remote, reasonably possible and probably.
- Significance: Management's assessment of the significance of a fraud risk should include not only financial statement and monetary significance but also significance to criminal, civil, and regulatory liability. The recommended grading categories include immaterial, more than significant, and material.

CIMA (2009, p.20) says as part of the Risk Management Cycle, the Fraud Risk Assessment & Management Team should understand and assess the scale of risk in the initial stages itself. The group should agree on the most appropriate definition and number of categories used when assessing likelihood and impact, the two variables normally used to assess the scale of risk. The assessment of impact should be on an overall basis, taking into account financial impact, political and commercial sensitivities, as well as the organizations viability and reputation. The analysis should be either qualitative or quantitative and should be consistent to allow comparisons. The qualitative approach usually involves grading risks in high, medium, and low categories. The assessment of the likelihood of a risk occurring is by using the below basis:

- Gross: Assesses the inherent likelihood of the event occurring in the absence of any processes, which the organization may have in place to reduce that likelihood.
- Net: Assesses the likelihood, taking into account current conditions and processes to mitigate the chance of the event occurring.
- Target: Likelihood of a risk occurring reflects the risk appetite of the organization

Curtis (2008, p.131) is of the view that risks are to be analyzed by considering the likelihood and impact as a basis for determining how they should be managed. CIMA, in the paragraph above, recommends that risks be assessed on an inherent and residual basis.

Therefore, all three references agree that two main variables (impact or significance and likelihood) are required to understand and assess the scale of risk. This paper shall follow the general recommendation of the references and use the qualitative approach of providing a range following a grading of high, medium, and low as compared to the recommendation of CIMA to use either quantitative grading. The assessment of the scale of risk is on an inherent and residual basis, taking into account the risk appetite ascertained. The assessment of the FRAM Team should be flexible yet detailed, taking into account industry expectations and externalities.

2.10. DEVELOPING A RISK STRATEGY

After assessing and identifying the possible fraud risks, the next step would be to develop a risk response

strategy. CIMA (2009, p.19) categorizes Risk Response Strategies to generally fall into one of the following categories:-

- Risk Retention (e.g. choosing to accept small risks)
- Risk Avoidance (e.g. stopping sale of certain products to avoid the risk of occurring)
- Risk Reduction (e.g. through implementing controls and procedures)
- Risk Transfer (e.g. contractual transfer of risk such as transferring risks to insurers).

Curtis (2008, p.131) mentions that Committee of Sponsoring Organizations of the Treadway Commission (COSO) also categorizes risk responses in the same way (avoiding, accepting, reducing or sharing risk) and sets to develop a set of actions to align risks with the entity's risk tolerances and appetite.

After deciding on the risk strategy, the final step shall be to implement, communicate, monitor and carry out periodic evaluation of the risk of fraud and controls in line with the dynamic changes in the organizations industry and business environment, and to assess it against the current risks identified and controls in place, in line with the recommendation by CIMA and Committee of Sponsoring Organizations of the Treadway Commission (COSO).

2.11. HYPOTHESIS AND RESEARCH QUESTION DEVELOPMENT

Coram et al (2008, p. 557) suggest that organizations with an internal audit department are more likely to detect and self–report fraud, especially those that do not outsource that function. However, for those organizations that are small and medium sized, it may not be feasible or cost efficient for them to have an Internal Audit Department. Therefore, it would be better to have an in house management team to monitor, test, and implement internal controls for small and medium sized companies who do not have the financial means to employ an internal auditor, set up an audit committee, or hire an external auditor to carry out an in-depth testing periodically.

In the literature review, a crucial step in identifying the required Internal Controls is to carry out a Fraud Risk Assessment and Management. This is to ensure that the identified Internal Controls are effective and would not cost the company in terms of inefficiency by implementing unnecessary controls.

Therefore, the Research Question (RQ1) and Hypothesis (H1) developed were as follows:

RQ1: Can Small and Medium Sized Organizations that carry out Fraud Risk Assessment & Management In House identify and implement effective Internal Controls which are in line with the Organizations risk appetite and strategy whilst not compromising on the efficiency of operations?

H_1: Small and Medium Sized Organizations that carry out Fraud Risk Assessment & Management In House are able to identify and implement effective Internal Controls which are in line with the Organizations risk appetite and strategy whilst not compromising on the efficiency of operations .

3.0. RESEARCH DESIGN & METHODOLOGY

3.1. RESEARCH METHODOLOGY

The researcher's main criteria when selecting the research methodology is as follows:

1. Ability to carry out an in-depth study of all documents, employees, culture, environment and processes without any limitations.
2. To be able to carry out the necessary steps to test the current internal controls, environment and to participate in discussions and decision making process.
3. To be able to bridge the gap between theory and practise, and to produce an actual process flow which reflects the true professional practical situation.

Therefore, the research methodology selected by the writer of this thesis was to use Action Research with a Case Study to be able to achieve the above. The writer agrees with Kizito and Kuhne et al (1997, p.23), whereby that Action Research enables research to take place in real life situations and to solve actual problems or issues, rather than just taking a more theoretical method. Since the focus of this paper was not on the general practice, or whether the preferred choice was to use Internal Auditors or External Auditors etc, the writer did not feel it was necessary to carry out a survey or to interview other organizations. Apart from the time constraint, the other reason was the writer chose to use purposive sampling to ensure a more in-depth research to achieve the objectives of this paper. The case study is on a Community Manager, whereby a Fraud Risk Assessment Team consisting of managers managing the organization was set up. Brainstorming sessions were carried out between the two Finance Managers, and also included meetings and interviews with other Process Owners from Purchasing, Contracts, and the Technical Team.

3.2. ACTION RESEARCH & CASE STUDY: COMMUNITY MANAGER

The organization selected was that of a Community Manager which the writer of this paper had access into the information, process and documents and was authorized to set up financial policies and procedures for the Community Manager. Due to the sensitivity of the case, the country, the organization or the individuals involved

will remain anonymous. However, the main essence of the case study, the actual interviews, minutes of meetings, brainstorming sessions within the key management team and other documents remains the same.
The key criteria's for selecting the Community Manager:

1. An organization which is relatively new, small and fast progression planned.
2. Focus on optimisation of funds and clear policies
3. An environment with non stringent rules and regulations
4. Cash flow and financial issues related to fast paced growth. This was a key requirement, as the writer agreed with Johnson (2008) that the temptation to commit fraud would be higher in a financially troubled company.

4.0. ANALYSIS & RESULTS

As defined by Wikipedia, a Community Manager is a manager of a "condominium or homeowners association including single-family home subdivisions, townhouses, or mixed-use development". Although Wikipedia is not a verified source, this definition of the role of a Community Manager is in line with the writer's experience of being involved with the Community Manager in the said case, as well as what is described in the governing documentation of the mentioned Community Manager. Hyatt (1975) agreed with the above definition and scope. The Community Manager in this region is not a recognized legal entity as there is no law governing its incorporation or running.

The selected Community Manager manages a mixed-use development (hereinafter known as the Community), whereby they collect monthly charges (known as Service Charges) from the unit owners and disburse it for the maintenance and improvement of the common use facilities in the Community. The Community Owners (Developer) hires the Community Manager as an Agent. A more in depth explanation about the role of the Community Manager is discussed later in the paper. The data collection methods would also include brainstorming sessions, meetings, and discussions with the key members / managers of the Community Manager.

The reason why the writer selected the particular Community Manager as a case study apart from the reasons above was:-

- As mentioned, the Community is NOT a legal entity and not registered with any governing body; hence, its bank accounts and financial statements etc are held and managed by the Community Manager, who is a legal entity. However, due to the lack of accountability and legal restraints, the risk of fraud happening here is relatively high.
- There is no defined and approved strata law yet in place to govern the running of the Community however for the time being, it is as an accepted practice to run it based on the terms of the Agreements until a proper law is in place.
- The writer had carried out an initial study which showed that there were red flags to denote a high possibility of fraud since there were apparent lack of controls or the controls were easily overridden by certain individuals

The flow of this section would be in the same flow as the steps identified under the Academic Literature to carry out a successful Fraud Risk Assessment & Management:
Steps:

1. Management to initiate the Fraud Risk Assessment & Management by setting up a Fraud Risk Assessment & Management Team (FRAM Team) and to set goals ,objectives to be met and the risk appetite of the organization.
2. FRAM Team to carry out brainstorming activities and discussions / interviews with other personnel to understand the following:
    - 2.1 The organizations environment, management, business, departments, processes , functions and owners
    - 2.2 Potential fraud scenarios and schemes, taking into account red flag areas such as management override of controls and personnel who may have the three factors identified in the Fraud Triangle – Opportunity, Rationalization and Motivation
    - 2.3 Identify the categories required and assess the likelihood and impact of the fraud schemes accordingly
    - 2.4 Based on the above, do a review and gap analysis of the current controls in place and any additional or revised controls needed, in line with the organizations risk appetite and decided risk strategy

The above steps showed that Small and Medium Sized Organizations that carry out Fraud Risk Assessment & Management In House are able to identify and implement effective Internal Controls which are in line with the Organizations risk appetite and strategy whilst not compromising on the efficiency of operations, therefore proving both the hypothesis and research question right.

4.1 FRAUD RISK MATRIX OR RISK REGISTER (Extract)

Table 1: Fraud Risk Matrix Or Risk Register For Company X

FACTOR / RISK AREA	DEPT.	LIKELI-HOOD	IMPACT	INTERNAL CONTROLS IDENTIFIED
ASSET MISAPPROPRIATION				
Receipt Schemes				
Skimming - Unauthorized taking of cash /cheques before recording revenues or receivables (or understating cash or receivables) - off book funds	Finance	Medium	High	Ensure separation of duties and access control between *Cashier *Personnel who prepare the bank deposit.

5.0. CONCLUSION.

Setting up Internal Controls and a Control Environment to prevent fraudulent activities in an organization can only be taken seriously when the tone is from the top. Until the committee was set up to oversee the management of the Community, there was a lot of conflict and attempts to override the controls set in place, even though the Finance Managers had already set up some interim controls.

The success of identifying the Internal Controls largely depended on the structured yet flexible approach taken by the FRAM Team. Otherwise, many controls would have been introduced that would have increased the bureaucracy of operations and increase of cost, and would have cost the company highly in terms of efficiency and effectiveness.

The steps followed were extremely crucial to identify key areas and red flags to prioritize the controls needed. By setting up the team, and ensuring their goals were in line with the vision and mission of the company was a strategic plan by itself. By doing so, the organization was able to incorporate the controls as part of their Key Performance Indicators and as part of their operational processes. By identifying their risk appetite, the team would also know what to focus on especially due to the time constraint faced.

By identifying the processes, functions, departments etc, the FRAM Team were able to understand better the loopholes and opportunities to commit fraud within the organization, especially since they were both new to the organization and industry. Since there was involvement of the personnel from all the other department and functions, the Fraud Risk Assessment was a good communication tool that informed the personnel that the organization was being serious about having a zero tolerance for fraud.

Having placed a grade on the various scenarios and possibilities identified, it then helped the FRAM Team to place more emphasis on those areas, which especially had high impact and high likelihood. Hence, more controls were placed in those areas. Therefore, the hypothesis was proven correct, that by following the steps outlines in the Literature review, the FRAM Team was able to come up with Internal Controls, which were deemed effective and efficient. A week of monitoring after implementing the controls found that lesser documentation was required, and the processing time was lowered. However, the study and monitoring of the newly implemented Internal Controls was not carried out as part of the scope in this paper and is recommended to be carried out in the future as a separate study.

The above process will be repeated periodically to review the controls set in place, and the effectiveness of the controls in view of future transactions, management directions, and technology improvement. As mentioned, this is a major process that needs to be undertaken by the management on an annual basis; ensuring proper resources are allocated for the successful implementation of the same, and should be seen as part of their goals to be achieved.

There does not seem to be a one-size fit all solution here. It is best to keep a flexible approach as it tailors makes the final controls to suit the organization and its processes.

6.0. REFERENCES

ACFE: ASSOCIATION OF CERTIFIED FRAUD EXAMINERS (2010), *Report To the Nation 2010* (http://www.acfe.com/rttn/2010-highlights.asp - last viewed on 8/1/2012)

AICPA et al (2008), *Managing the Business Risk of Fraud: A Practical Guide* (http://www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/FraudPreventionDetectionResponse/DownloadableDocuments/managing_business_risk_fraud.pdf - last viewed on 08/08/2012)

AUDITING STANDARDS BOARD (2002) Statement on Auditing Standards No.99: Consideration of Fraud in a Financial Statement Audit, AICPA

ALLEN ROBERT D et al (2006), "Auditor Risk Assessment: Insights from the Academic

Literature",*Accounting Horizons*, pp. 157
AUDITING AND ASSURANCE STANDARDS BOARD 2006, *AUSTRALIA AUDITING STANDARD ASA 240, "The Auditor's Responsibility to Consider Fraud in an Audit of a Financial Report"*
BARAC KARIN et al (2010), "Internal Audit Outsourcing Practices in South Africa, *African Journal of Business Management Vol 3 (13) 2009*, pp 969-979
BEASLEY MARK S et al (2003), "A Primer for Brainstorming Fraud Risks", *Journal of Accountancy ,* pp.1-12.
BERAN DENNY et al (2009), "Fraud Risk Assessment Enterprise Wide Risk Assessment", *Corporate Compliance Insights.Com* (http://www.corporatecomplianceinsights.com/managing-corporate-risk-fraud-risk-assessment-enterprise-wide-risk-assessment/- last viewed on 8/1/2012)
CIMA: CHARTERED INSTITUTE OF MANAGEMENT ACCOUNTANTS (2009), *CID Tech Guide: Fraud Risk Management* (http://www1.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf - last viewed on 18/12/2011)
COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION -COSO (2012), *Enterprise Risk Management – Understanding and Communicating Risk Appetite*
COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION -COSO (1987), *Report of the National Commission on Fraudulent Financial Reporting*
CORAM PAUL et al (2007), "Internal Audit, alternative Audit Structures and the level of misappropriation of assets fraud", *Journal Compilation Accounting and Finance Association of Australia and New Zealand, 2008, pp* 553-559
EUROPEAN COMMISSION RECOMMENDATION (2003), *Definition of Small and Medium Sized Enterprises*
HYATT WAYNE S (1975), Condominium and Home Owner Associations: Formation and Development
JOHNSON SARAH (2008), "Deloitte study sees fraud ties to bankruptcy". *CFO.com*, (http://www.cfo.com/printable/article.cfm/12671294 - last viewed on 12th August 2012)
KIZITO F (-), Sustaining The Benefits Of Action Research In Decision Support Tools Development pp. 37-41
KPMG (2006), *Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response* (http://www.amr.kpmg.com/aci/docs/fraud_risk/Fraud_Risk_Web11_01_06.pdf - last viewed on 18/12/2011)
KUHNE, G.W. et al (1997) "Understanding and using action research in practice settings" *New Directions for Adult and Continuing Education,* no. 73.(pp 23-40)
KUMAR RANJIT (2005), *Research Methodology-A Step-by-Step Guide for Beginners*,(2nd.ed.), Pearson Education
LENARD M.J et al (2009), "An Historical Perspective on Fraud Detection: From Bankruptcy Models to Most Effective Indicators of Fraud in Recent Incidents", *Journal of Forensic & Investigative Accounting,* Vol 1, Issue 1, pp. 1 - 27
NDSG: North Dakota State Government (-), *Fraud Risk Assessment Guideline* (http://www.nd.gov/fiscal/docs/fraudriskdocumentwithappendix.pdf - last viewed on 18/12/2011)
O' BELL ERICK (2009), "5 Anti Fraud Strategies to Deter, Prevent and Detect Fraud", *Corporate Compliance Insight* (http://www.corporatecomplianceinsights.com/2010/internal-control-checklist-deter-prevent-detect-fraud -last viewed on 8/1/2012)
PWC: PricewaterhouseCooper's (2007), *Global Economic Crime Survey in 2007 (*http://www.pwc.com/gx/en/economic-crime-survey/pdf/pwc_2007gecs.pdf - last viewed on 18/12/2011)
PWC: PricewaterhouseCooper's (2009), *Global Economic Crime Survey in 2009* (http://www.pwc.com/gx/en/economic-crime-survey/assets/global-economic-crime-survey-2009.pdf - last viewed on 18/12/2011)
RIKHARDSSON PALL et al (2006), "Business Process Risk Management and Internal Control: A proposed Research Agenda in the context of Compliance and ERP systems" in Proceedings Second Asia/Pacific Research Symposium on Accounting Information Systems, Melbourne. (http://eprints.qut.edu.au/5192/1/5192.pdf - last viewed on 11/02/2012)
ROGGEVEN L.L. (2009), "Are auditors more alert on fraud?" Erasmus University Rotterdam
RUIN JOSEPH EBY (2009), *Internal Auditing: Supporting Risk Management, Fraud Awareness Management and Corporate Governance*, Leeds Publications.
SHANMUGAM JAYA KUMAR et al (2012), "An Exploratory Study of Internal Control and Fraud Prevention Measures in SME's"
TURNER JERRY L et al (2003), "An Analysis of the Fraud Triangle", pp 1 - 33
U.S. SECURITIES AND EXCHANGE COMMISSION, SARBANES OXLEY SECTION 404 – A Guide for Small Business
VERSCHOOR CURTIS.C. (2008), *Audit Committee Essentials*, John Wiley & Sons
WAGNER STEPHEN (2006), The Unexpected Benefits of Sarbanes-Oxley, Harvard Business Review 2006, pp

1 - 10
WELLS JOSEPH T. (2007), *Corporate Fraud Handbook – Prevention and Detection, 2nd Edition*, John Wiley & Sons
WIKIPEDIA (-), *Definition of Community Manager (*http://en.wikipedia.org/wiki/Community_manager - last viewed on 18/12/2011)
YALE UNIVERSITY AUDITING, *Balancing Risks and Controls*

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/

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