# Managing the Occupational Fraud : A Proactive Approach*

## 직무부정의 관리: 예방적 접근 방법

Lee, Gi Youl(이 기 열)**

ABSTRACT

미국의 공인부패조사위원회(ACFE)는 "2008년 직무부정과 남용" 이라는 보고서에서 미국 기업은 년 평균 매출액의 7%를 부정에 따른 손실로 예측하며, 이는 국내총생산대비 $9940억에 이를 것으로 추정하고 있다. 기업의 부정은 크게 경영자의 부정과 종업원의 부정으로 구분할 수 있다. 기업의 소유주인 주주들의 부를 관리, 증진시키도록 수탁책임을 부여 받은 경영자는 그들의 의무를 신의 성실하게 수행하고 그 결과를 투명하게 보고할 책임이 있으나, 기업이 처한 대내외적 환경 도는 개인적인 욕심으로 인해 부정을 저지르곤 한다. 종업원의 부정은 흔히 기업자산의 횡령이나 착복으로 나타난다. 그러나 부정의 원인이 누구에게 있던 지간에 부정은 허위재무보고를 동반하며, 이는 기업의 재무보고서에 대한 신뢰성의 상실을 야기 시킨다. 이 신뢰성의 상실은 기업 회계정보이용자의 합리적인 의사결정을 방해하며, 이는 결과적으로 금융시장의 쇠퇴를 야기 시킬 수 있다. 기업의 부정은 부정에 연루된 기업뿐만 아니라 부정에 연루되지 않은 기업까지도 자본비용을 증가시켜, 이는 결국 선량한 소비자들의 부담이 된다. 기업의 부정이 사회전반에 미치는 파급효과는 실로 엄청나다고 할 수 있다. 그런데 문제는 부정의 적발이 쉽지 않으며 내부 및 외부감사도 감사자체의 본질적인 한계로 인해 실제 적발한 부정건수는 빙산의 일각에 불과하다는 것이다. 따라서 부정의 예방이 적발보다 효과적이며, 이를 위해서는 내부통제제도가 잘 되어 있어야 한다. 그러나 내부통제가 본래 의도된 목적을 달성하기 위해서는 기업의 지배주체(governing body)가 환경과 여건을 조성해야 한다.

Key Words : Occupational Fraud(직무부정), Fraud Schemes(부정책략), Internal Control(내부통제), Corporate Governance(기업지배구조)

* The present research was conducted by the research fund of Dankook University in 2008.
** Professor of Dankook University , College of Economics and Business

## I. Introduction

Occupational fraud is to defraud the employing organization through the deliberate misuse or misapplication of the organization's assets for personal enrichment. Occupational fraud ranges from simple petty cash theft to sophisticated investment swindles. Recent example includes the prominent trader, Bernard L. Madoff. he legendary trader on Wall Street was arrested at his luxurious Manhattan home by the U. S. Federal agents with accusation of multi-billion dollar investment fraud scheme, even though the exact magnitude of the fraud has yet to be determined. But the criminal indictment filed against him estimated $65 billion in loss. Bernard L. Madoff's Investment Security, the firm that he founded in 1960, operated more than 20 funds by managing $17 billion. Those funds lured investors, hedge funds, and institutional customers for more than a decade with the rosy promise of high returns and low fees.

Investors sought Mr. Madoff out to have their monies managed to reap the steady and solid returns. One of those funds, the Fair Field Security Fund, reported $7.3 billion in assets and claimed to have paid more than 11 percent interest each year for the past 15 years since its inception. Paying too much interest even during the market volatility period drew skepticism among many fund managers, because the fund's performance was too good to be true. Struggling to raise $7 billion to cover client's withdrawal, Mr. Madoff finally confessed that his money-management business was "all just one big lie" and "basically a giant Ponzi scheme."[1] Even before surrendering himself to the authority, he tried to distribute $200 million to $300 million to certain employees, family and friends rather than paying back those monies to his fraud victims. Many of his victims included well known celebrities and organizations, such as Steven Spielberg, Larry King, the Spitzzers and Yeshiva University. It appears that anyone having money would be his potential target. The fraudster's lies were translated into half-dozen languages, resulting in the victims scattered from Holly Wood to Abu Dhabi. On June 29, 2009, Bernard Madoff was sentenced to 150 years in prison, the maximum sentence and fined $ 170 billion in restitution. The lesson from this fraud scheme is "when money goes global, fraud does, too."[2]

The Association of Certified Fraud Examiners (ACFE, 2008) reported in its

1) www. washiontonpost.com/wp-dyn/content/article/2009/02/28/AR2009022801801905.htm
2) www.iht.com/articles/2008/12/21/business/madoff.php

"2008 Report to the Nation on Occupational Fraud and Abuse" that U. S. companies might lose 7 percent of their annual revenues due to fraud. By applying 7 percent to the projected 2008 U. S. Gross Domestic Product (GDP), about $994 billion was vanished due to fraud.[3] ACPE (2008) drew the following findings from the study based on data compiled from 959 cases that were investigated between January 2006 and February 2008 by the Certified Fraud Examiners (CFEs):

- The typical fraud lasted two years from its inception until the time it was caught.
- Despite emphasis to strengthen internal controls by Sarbanes-Oxley Act, the data how that occupational fraud is more likely to be detected by tips rather than udits or internal control procedures. The report shows that 46 percent were detected by whistle blowing tips from employees, customers, vendors, and others.
- The report shows that the industries most vulnerable to fraud are banking and financial services (15%), government (12%), and healthcare (8%). It also shows that small businesses are more vulnerable than large ones.
- Lack of adequate internal controls was cited as the main reason for occupational fraud. Lack of management review and its override over internal control were also cited as causes for fraud.
- Accounting department personnel and upper management perpetrated fraud (29 percent for accounting personnel and 18 percent for management) than any other lines of organization's hierarchy. But the magnitude of fraud committed by management far exceeded those committed by employees.

Occupational fraud causes serious financial problems not only to those organizations victimized, but also creditors and other stakeholders. In addition, many instances of fraud went undetected because of ineffectiveness of internal control system and inherent limitations of internal and external audits. That is the reason that the occupational fraud is more likely to be detected by tips from various sources. Even for those detected, the full amount defrauded may not be ascertainable. Determining the true breadth and depth of the fraud is extremely difficult, if not impossible. Hence, the current study purports to provide the

3) The U. S. Chamber of Commerce estimates that the annual cost of fraud exceeds $100 billion. On the other hand, the General Accounting Office (GAO) projects that fraud costs the U. S. government almost $100 billion annually. This figure combined with the U. S. Chamber of Commerce's estimate represents total cost of more than $200 billion to the society. Browning and Dugan (2002) estimated that management fraud have cost to investors close to $7 trillion.

system-wide framework to deter or prevent occupational fraud rather than ways to detect the fraud.

Fraud can be perpetrated by any person in the organization. But regardless of who commits fraud, fraud has more remote and dangerous impact on the capital markets: loss of public confidence in the fairness of financial information. Public's confidence in the fairness of financial reporting is essential to the effective functioning of the securities market. But the loss of public confidence will increase the cost of capital even to those companies not involved in corporate fraud, which eventually results in improper functioning of the securities market.

The remainder of paper is organized as follows: Occupational fraud, its environment, and symptoms are discussed in section II, followed by fraud schemes in section III. Section IV will discuss the ways to fight fraud, followed by conclusion in section V.

## II. Occupational Fraud, Fraud Environment and Symptoms

### 1. Occupational Fraud

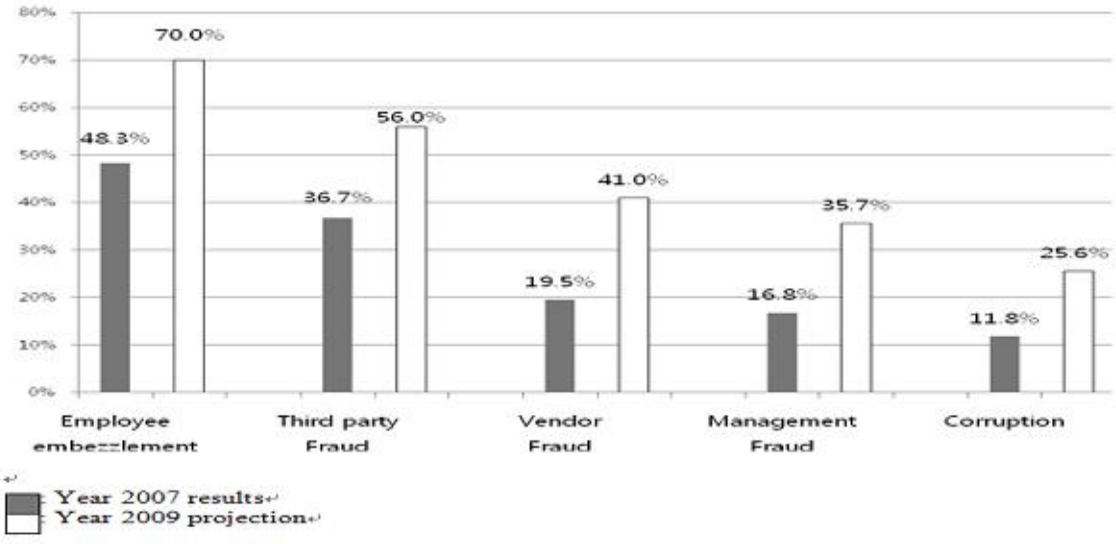
Occupational fraud, depending on who commits fraud, can be categorized as management fraud or employee fraud. Management fraud, often called fraudulent financial reporting, is committed by management for the purpose of window-dressing financial statements. Two most common techniques used by management involve improper revenue recognition and overstatement of assets.

According to the study done by Committee of Sponsoring Organizations of the Treadway Commission (COSO), 50 percent of U. S. companies which committed financial statements fraud between 1987 and 1997 recorded revenues prematurely or created fictitious revenue transactions. In addition, 50 percent of the fraud companies overstated assets by means of overvaluing existing assets, recording nonexistent assets, or capitalizing items that should have been expensed. Typically overstated assets include inventory, net accounts receivable due to understated allowance for doubtful accounts, and fixed assets. The COSO reports that the median fraud amounted to $4.1 million, which is relatively large considering total asset of $15.7 million of the median company. The chief executive officer (CEO) and/or the chief financial officer (CFO) committed 83 percent of the fraud cases.[4] Motivations behind management fraud were to avoid loss, to increase stock price, or

to meet stock analysts' expectations. The officers and members of the board of directors were also financially motivated to commit fraud, because they owned 32 percent of the company stocks. Payoffs of the management fraud were significant in that more than a half of the companies filed bankruptcies or were under substantially different ownerships.

On the other hand, employee fraud, often called misappropriation of assets, embezzlement or defalcations, is to misuse or misappropriate the company's assets. Employee fraud can be either direct or indirect. Direct fraud occurs when an employee steals company properties, such as cash, inventory, supplies, or other assets. Indirect fraud occurs when employees take kickbacks or bribes from vendors, customers, or any one outside the organization. Types of employee fraud include skimming, cash larceny, billing schemes, payroll schemes, expense reimbursement and misappropriation of non-cash assets. Employee fraud usually benefits the individual perpetrator, while management fraud benefits his/her company and officers by deceiving investors and creditors through fraudulently reporting financial statements. But management fraud is more difficult to detect than employee fraud, because management is in a position to alter, falsify, or create source documents by collusion with employees or third parties. Figure 1 shows types of fraud incidents in 2007 and fraud projections in the coming year.

Figure 1. Types of fraud incidents, source: ACFE (2008)




4) Refer to the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) 1999 analysis of cases of fraudulent financial statements investigated by the U. S. Securities and Exchange Commission (SEC).

## 2. Fraud Environment

Three elements to fraud environment are perceived pressure, perceived opportunity, and rationalization. Figure 2 shows the fraud triangle representing three elements.

Figure 2. Fraud Triangle


Albrecht et al. (2009) identified perceived pressure as the one that motivates individuals to commit fraud such as financial pressure, vices, or work pressures. Individual financial pressure may come from personal greed, living beyond one's means, extreme personal debts, or unexpected financial needs. Corporate financial pressure, such as poor cash position, uncollectible receivables, loss of customers, obsolete inventory, or declining market condition, often motivates management to fraudulently report financial statements. Vice pressures, such as gambling, drugs, and alcohol, may also induce individuals to perpetrate fraud. But other factors, such as little recognition for job performance, job dissatisfaction, being overlooked for promotion or being unpaid, also entice individuals to commit fraud.

The second element is a perceived opportunity to commit fraud. For example, factors such as lack of effectiveness of internal control, inability to judge quality of performance, failure to discipline fraud perpetrators, and lack of audit trail, contribute fraud opportunities. Establishing an effective internal control system is the crucial step to deter and detect employees' wrong-doings. Many frauds were perpetrated in environments in which control system was supposed to be in place, but it was not. Section IV will discuss further details of preventive measure to fraud. An ordinary person is unable to evaluate the quality of the professionals' job performance. When those professionals were faced with the

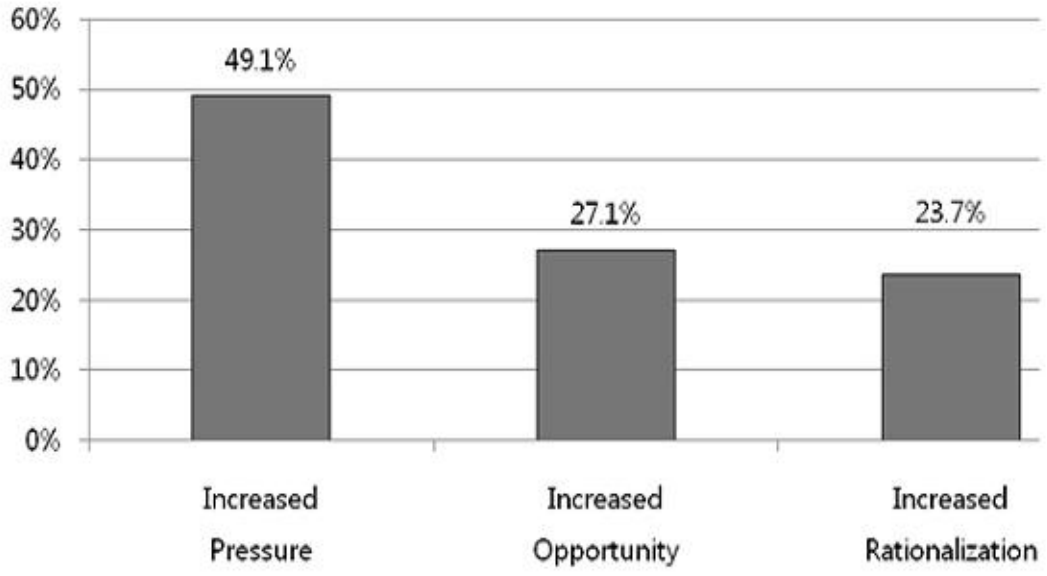
pressure to cheat and believed that their customers would not know what they have done, they would commit fraud. If the fraud perpetrators were not punished or marginally sanctioned for what they had done, they might resume those behaviors again.

As for the third element, human beings have tended to rationalize their behavior, such as rationalization for not exercising enough, for being overweight, and for spending more than they earned. Unfortunately, people rationalize their dishonest behaviors for them not to feel guilty. Common rationalization that perpetrators use includes the following:

- The company owes it to me.
- I only borrow money and will pay it back.
- Nobody gets hurt.
- It's for good purpose.

Albrecht et al. (2009) suggests that three common fraud elements must be present for fraud to be committed: a situational pressure (non-shareable financial pressure), a perceived opportunity to commit and conceal the dishonest act (a way to secretly resolve the dishonest act), and some ways to rationalize the act contrary to a perpetrator's conscience level. Figure 3 shows the percentage of each contributing factor to fraud.

Figure 3. Contributing Factors Prompting to Commit Fraud, source: ACFE (2008)



### 3. Fraud Symptoms

Albrecht et al. (2009) listed the ten most motivating factors for individual to commit fraud as:

a) Living beyond one's means
b) Overwhelming desire for personal gain
c) Too much personal debt
d) Close association with customers
e) Feeling that salary was not commensurate with the performance
f) A wheeler-dealer attitude
g) Strong desire to beat the system
h) Excessive gambling habits
i) Undue family or peer pressure
j) No recognition for job performance

At the same time, the ten most highly ranked motivating factors for organizational environment are:

a) Placing too much trust to key employees
b) Lack of proper authorization procedures for transactions
c) Inadequate disclosure of personal investments and incomes
d) No separation of duties between authorization of transactions and custody of assets
e) Lack of independent checks on performance
f) No separation of duties between custody of assets and accounting for them
g) Inadequate attention to details
h) No separation of duties among accounting functions
i) Lack of clear lines between authority and responsibility
j) No review by internal auditors

Because it is almost impossible to totally eliminate motivating factors, the current study focuses on system-wide approach to alleviate the fraud opportunities in the organizational environment. Fraud schemes are discussed in the next section.

## III. Fraud Schemes

ACFE (2008) mentioned that misappropriation of assets accounted for

approximately 90 percent of occupational fraud. The misappropriation schemes can be further broken down into skimming, cash larceny, billing scheme, check tampering, expense reimbursement, payroll schemes, and misappropriation of non-cash assets.

Skimming and cash larceny are perpetrated against organization's incoming receipts. Skimming is any scheme in which cash is taken before being recorded on the company books and records. It is known as "off-book" fraud and difficult to detect, because it never leaves an audit trail. An example is when employee pockets cash payment from a customer without recording a sale. Skimming accounts for about 17 percent in misappropriation of asset cases. On the other hand, cash larceny occurs when cash is stolen after being recorded on the books. An example is embezzling cash and checks from daily receipts before being deposited to a bank. Cash larceny is relatively easy to detect than skimming, because it leaves an audit trail. It accounts for 10 percent of all fraud cases.

In a billing scheme, the perpetrator induces his/her employer to issue a payment for fictitious goods, services, or inflated invoices. Billing scheme can be sub-categorized into shell company scheme, non-accomplice scheme, and personal purchase scheme. In a shell company scheme, the fraudster approves fraudulent invoices for nonexistent services by a shell company which is a fictitious entity created for the sole purpose of committing fraud. An example of non-accomplice vender scheme is as follows. A secretary responsible for opening mail, processing claims and authorizing payments intentionally pays a legitimate bill twice. Then she would request the recipient to return the overpaid amount, and intercept and deposit the returned check in her own account. In this example, perpetrator made fraudulent disbursement for the invoice of a non-accomplice vendor. Billing schemes account for about 24 percent of all fraud cases. Instead of undertaking billing schemes, many fraudsters simply purchase their personal items with company credit card.

Check tampering is another type of fraudulent disbursement in which the perpetrator converts company funds to his own by forging, altering, or stealing a check the company has drawn. It accounts for about 15 percent of all fraud cases. Expense reimbursement scheme is a very common form of occupational fraud and extremely difficult to detect. It occurs when employees make false claims for reimbursement of fictitious business expenses or pad the amount of business expenses incurred to generate excess reimbursements. It accounts for 13 percent of all fraud cases. Payroll scheme occurs when employee claims overtime payment for

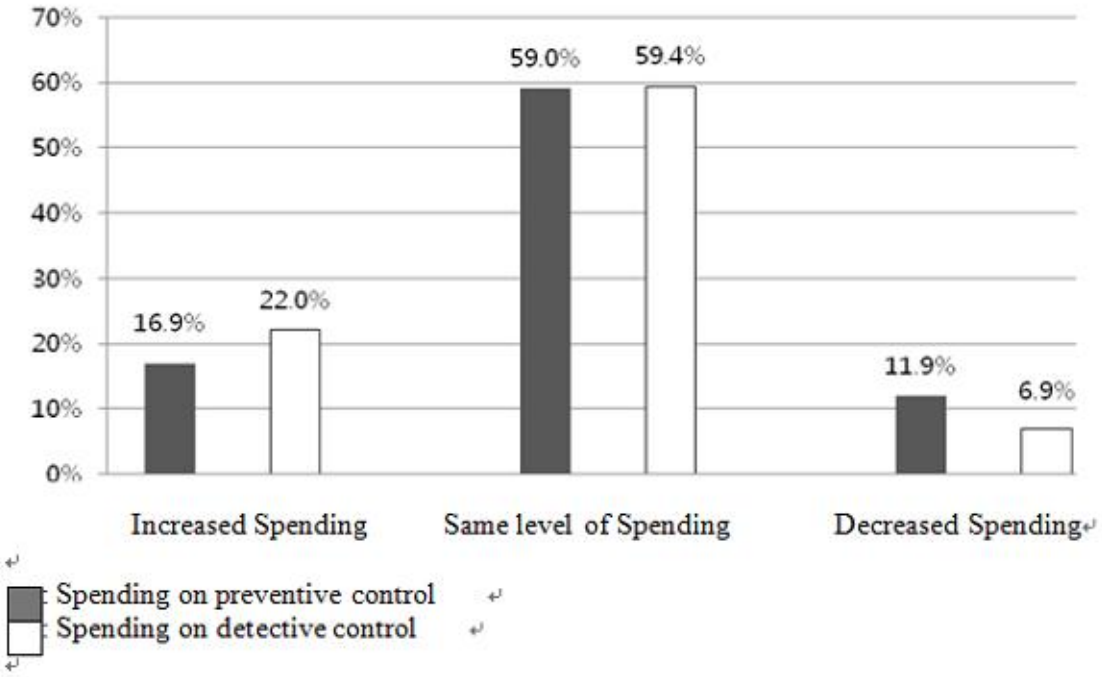
hours not worked or adds nonexistent (ghost) employees to the payroll. It accounts for 9 percent of all fraud cases.

While most of asset misappropriation scheme relates to cash, other assets can be stolen as well. Stealing inventory from a company's warehouse is an example of non-cash asset misappropriation. An employee who takes company vehicles for personal use misuses the company asset. Even though the vehicle was returned unharmed and the cost to the company was only minimal, unauthorized use of a company asset was tantamount to fraud when a false statement on the usage of the company vehicle was accompanied. Non-cash asset misappropriation accounts for 16 percent of all fraud cases. Next section discusses the features of internal control system as a means to deter and detect occupational fraud.

## Ⅳ. Ways to Fight Fraud: Preventive Controls

Of the 507 Chief Financial Officers (CFOs) who responded to the ACFE (2008) survey, 51.5 percent realizes the necessity to combat fraud, especially in the financial distress era. But on the contrary to their belief, many organizations are cutting budgets and tightening their spending on fraud deterrent system. As figure 4 has shown, 59 percent of respondents indicated that their companies have maintained the same level of spending as past year on preventive measures for fraud. On the other hand, only 17 percent have increased their spending on preventive controls. Compared to spending on preventive controls, spending on detective controls was increased in the economic downturn periods. Considering the nature of fraud and difficulty to detect, preventive measures are more effective means than detective measures for fraud deterrence.

Figure 4. Spending on Prevent and Detective Controls During 2008, source: ACFE(2008)




## 1. Objectives of Internal Control

The objectives of internal control are to provide reasonable assurance that:

a) assets are safeguarded and used for business purposes
b) accounting information is accurate
c) employees comply with laws and regulations.

Internal control can safeguard assets by preventing theft, fraud, misuse, or misplacement. Accurate accounting information is necessary for operating a business successfully. The safeguarding of assets and accurate accounting information often go hand in hand, because employees attempting to misappropriate assets or embezzle cash will also need to adjust accounting records to hide the fraud. In addition, business must comply with applicable laws and regulations and reporting standards. Examples of such laws and standards include environmental regulations, contract terms, and generally accepted accounting principles (GAAP).

## 2. Components of Internal Control

To achieve the objectives of internal control, management is responsible for designing and applying four components of internal control. These components are control environment, risk assessment, control procedures, and monitoring.

### 1) Control Environment

The control environment consists of the actions, policies, and procedures that reflect overall attitude of directors and top management about the importance of internal control to the entity. That is why the control environment is often referred to as the entity's tone at the top. If top management keeps telling about the importance of internal control, subordinates will tend to follow the established control. Without a solid control environment as a foundation, the other elements of internal control are not likely to function at its intended level. The following sub-components are the factors that influence the control environment.

(1) Management's Philosophy, Operating Style, and Code of Ethics

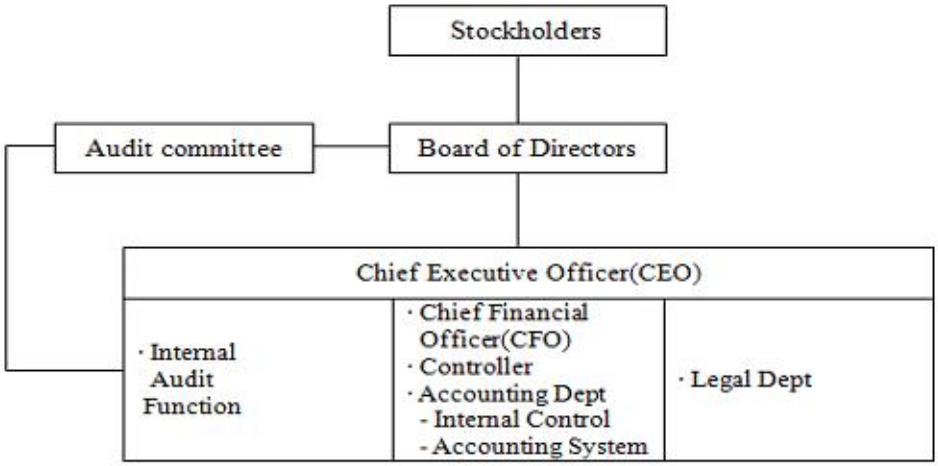
A management who often overrides control policies may indirectly encourage employees to ignore controls. Also, the management that overemphasizes achievement of target revenue may create undue pressures that may lead employees to fraudulently record sham sales. Management cannot act one way and expect others to behave differently. On the other hand, a management that emphasizes the importance of controls and encourage adherence to control policies will create an effective control environment. Corporate code of ethics is designed to provide guidance on employees' behavioral standards that must be observed while performing their duties. The code may accommodate the management's attitude to remove or reduce temptations that might lure employees to engage in unethical or illegal acts.

(2) Board of Directors and Audit Committee

Shareholders of a company normally do not exercise direct control over the operations of the company. Instead, they indirectly control the company through the election of a board of directors. The board of directors selects officers who actively manage the company, but must be independent of management. The reason is that the board was entrusted with authorities from shareholders to oversee management's activities for the protection of their wealth. The board advises and

approves strategies and operation of business as well as monitoring them. This system of authoritative directions is called corporate governance, which has a profound impact on the performance of business. Figure 5 depicts a general corporate governance structure related to financial reporting process.

Figure 5. Corporate Governance Structure
-Financial Reporting Process




The essence of the corporate governance is the board of directors, which sets and governs the directions, strategies, operation, and financial reporting. But the board delegates responsibilities for establishing and maintaining internal control procedures to management and, in turn, assesses its effectiveness. The board also monitors the possibility that the management overrides control policies. Since shareholders are not directly involved in day-to-day operations, they must rely on financial reports in evaluating management's performance. To get help for its oversight function over management performance and financial reporting, the board establishes an audit committee.

An audit committee is a selected number of the board of directors whose responsibilities include overall oversight function on financial reporting and internal control processes. In fulfilling these responsibilities, the audit committee considers the potential for management's override of internal controls and oversees management's fraud risk assessment. Audit committee's oversight function also serves as a deterrent to fraud. For example, audit committee's frequent contacts and open line of communication with auditors and all lines of management may

assist the committee to identify fraud attempts and to assess the strength and weakness of the internal control and the potential for the fraudulent financial reporting. The committee also helps the board discharge its fiduciary duties to shareholders satisfactorily by delivering information that it has acquired through the monitoring process to the board. The audit committee's involvements in the financial reporting process and frequent contacts with auditors are important determinants in evaluating proper functioning of internal control system and financial reporting.

(3) Personnel Policy

The most important factor for the control system to function at the level it was planned is personnel. Competent and trustworthy personnel enhance effectiveness of internal control, while incompetent or dishonest people may nullify the system to shambles. Personnel policy should be established to provide the entity with reasonable assurance that

- All new personnel should be qualified to perform their work competently and honestly.
- Work is assigned to personnel with adequate technical training and proficiency.
- Personnel selected for promotion has qualifications necessary to fulfill the assigned responsibilities.

### 2) Risk Assessment

All business entities face risks from external or internal environment. Risk may include deepened competition for market share, changes in consumer behavior patterns, regulatory changes, and interest rate change, and so on. Management should continually assess these risks and take necessary actions to cope with them so that the objectives

of internal control can be attained. Management also assesses risks as a part of implementation process to minimize fraud opportunities for the changing environment.

### 3) Control Procedures

Control procedures are policies to provide reasonable assurance that business goals will be achieved. The Institute of Internal Auditors' report (IIA, 2005) notes that control procedures generally relate to separation of duties, information

processing, physical controls, and performance reviews. More specifically, these procedures fall into the following five categories:

1. Adequate separation of duties
2. Proper authorization of transactions and activities
3. Adequate documents and records
4. Physical control over assets and records
5. Independent checks on performance

(1) Adequate Separation of Duties

To safeguard assets and ensure reliability of financial records, following guidelines must be observed.

i. Separation of the Custody of Assets from Accounting

To deter defalcations, a person in charge of custody of assets should not account for that asset. When one person is able to perform both functions, he/she can dispose of the asset for personal gains and alter the accounting record to hide theft. For example, if the accounts receivable clerk has access to cash receipts, the clerk can steal a customer's cash payment and then alter the customer's record to indicate the payment receipt. The customer would not complain and the theft would go undetected.

ii. Separation of Authorization for Transactions from the Custody of Related Assets

A person who authorizes transactions should not have access to the custody of related assets. For example, the person who authorizes the payment of a vendor's

invoice should not sign the check for the payment. If the same person does both functions, the possibility of defalcations may be significantly increased.

iii. Separation of Operational Responsibility from Accounting

The individuals responsible for sales should be separate from the individuals accounting for the receivables. By doing so, the accounting function serves as an independent check on sales. The employee who handles the accounting for receivable should not be assigned for collecting receivables. Separating these functions reduces the possibility of errors or fraud. In essence, the functions for operational responsibility, custody of assets, and accounting should be separated to reduce possibilities for occupational fraud. The accounting records then serve as an independent check on the persons who have custody of assets and those who are responsible for operations. For example, an employee who handles cash receipt

(custody of assets) should not record cash receipts in the accounting records (accounting). To do so would allow the employees to steal cash and hide theft in the accounting records.

iv. Separation of Responsibilities for Related Operations

To reduce the possibility of fraud, the responsibility for related operations must be divided. For example, responsibilities for purchasing, receiving, and paying for inventory must be separated. If the same person orders inventory, verifies the receipt, and pays for the invoice, the following wrong-doings could occur:

- Orders may be placed based on an intimate relationship with a supplier, rather than on price, quality, or other predetermined criteria.
- The quantity and quality of inventory received may not be verified with care, thus causing payment for inventory not received or deteriorated.
- The validity and accuracy of the invoice may be carelessly verified, thus resulting in the payment of bogus invoice.

(2) Proper Authorization of Transaction

Every transaction must be properly authorized. If any person can purchase or dispose assets at will, defalcations could result. Authorization can be either general or specific. Management establishes the level of general authorization for all subordinates to approve transactions within the limit set by the authorization level. Specific authorization applies to individual transaction, depending on the circumstance.

(3) Adequate Documents and Records

Documents and records are the source upon which transactions are based.

They include such diverse items as purchase orders, shipping documents, sale invoices, receiving reports, and others. Those documents perform to transmit information within or outside the entity. The documents and records must be adequate to control assets properly and to record transactions correctly. Documents and records should be:

- Pre-numbered consecutively to facilitate control over missing documents
- Prepared at the time a transaction takes place, or as soon as possible thereafter
- If longer time gaps between transaction and record date exist, records are vulnerable for modification or alteration.

(4) Physical Control over Assets and Records

Proofs and security measure should be used to safeguard assets and ensure reliable accounting data. If assets or records are not properly protected, they can be stolen, damaged, or altered. Physical precautions should be used to safeguard assets and records. For example, controls for safeguarding inventory include developing and using security measures to prevent damage or employee theft. Inventory must be stored in a warehouse or other place in which access is restricted to authorized personnel. The removal of inventory from warehouse must be accompanied by authorized requisition forms. The storage area must be locked when the business is not operating and climate controlled to prevent damage from heat or cold. Other examples are fireproof safes or safety deposit vaults to protect important documents and assets, such as title, currency and securities from fire, theft, or other mishap.

(5) Independent Checks on Performance

Independent checks on the procedures mentioned above are important, because existing control procedures tend to be changed or be neglected over time, unless frequent review is done. Humans tend to forget or fail to follow instructions due to carelessness, fatigue, or negligence, unless someone oversees their performance. But independent checks must be done by a person who did not participate in preparing the original data. For example, verification of bank reconciliation must be done by personnel who did not handle cash or accounting records.

**4) Monitoring**

Monitoring deals with ongoing or periodic assessment of the existing internal control to determine that the system is operating as is originally intended. Feedbacks for the assessment come from such diverse sources as studies on internal control, internal and/or external auditors' reports, or reports by regulations.

Monitoring may also involve observing employee behavior and warning sign of the accounting system. Bliss (1994) reports the following warning clues for people and accounting system:

Warning signs for people:

i) Abrupt change in life style(without causes such as winning the lottery)

ii) Close social relationships with suppliers

iii) Refusing to take vacations

iv) Frequent money borrowing from friends or colleagues

v) Excessive use of alcohol or drugs

Warning signs for the accounting system:

I) Missing documents (could mean documents were used for fraudulent transactions)

ii) An unusual increase in customer refunds (phony refunds)

iii) Difference between daily cash receipts and bank deposits (could mean pocketed before deposited)

iv) Abrupt increase in slow payments (employee may be pocketing the payment)

v) Backlog in recording transactions (possible attempt to delay fraud detection)[5)]

An organization's size has a significant impact on the internal control. It is obvious that a small company cannot afford to have internal auditors or establish adequate separation of duties. But even a small company can hire competent, trustworthy, and honest personnel. It can establish proper procedures for transaction authorization, execution, and recording. It can also have adequate documents and records, physical control over assets and records, and independent checks on performance. An owner's direct involvement in managing daily business can definitely be a plus to the control environment. An owner's close encounter with employees helps him evaluate the competence of the employees and enhances the effectiveness of overall system. For example, the effectiveness of internal control can be significantly improved if the owner signs outgoing checks after reviewing all supporting documents, reviews bank reconciliation, approves customer's credit, and bad debts.

## V. Conclusion

Fraud is any intentional wrongdoing aimed at deceiving others for the sake of personal enrichment. ACFE (2008) estimates that 7 percent of the U. S. Gross Domestic Product (GDP), which amounts to $994 billion, might be vanished due to fraud. Fraud can be perpetrated by management or employee. Management fraud,

5) Edwin C. Bliss, "Employee Theft," Boardroom Reports, July15,1994. pp.5-6

called fraudulent financial reporting, harms information users by providing incorrect financial statements information for their decision-making processes. Employee fraud, called misappropriation of assets, also hurts shareholders, creditors, and other stakeholders, because embezzled assets are no longer available to the rightful owners. Both types of fraud have detrimental impact on the transparency of financial statements. Widespread media attention to even a single incidence of corporate fraud can shake the public's confidence in the credibility of financial reporting, which may ultimately erode confidence of capital markets. Although eliminating fraud is a key consideration of every business, fraud increases both in frequency and amounts. The number of detected fraud incidents is likened to the tip of the iceberg. Most of fraud cases go undetected and its magnitude cannot be determined for sure.

Fraud occurs as the result of certain environmental, institutional, or individual forces and opportunities. Those forces and opportunities add pressures and incentives to businesses and individuals, and tempt them to engage in fraudulent activities. These temptations are present in all organizations and individuals to some extent. A proactive approach to lessen the tempting opportunities is the best way to manage fraud risks. The approach involves participation by all levels of personnel in the organization, including the board of directors, management, staff, internal and external auditors. The board's role is important, because it sets the general policies and strategies for the business operation. Vigilant monitoring on fraud risks sends clear signals to the public, stakeholders, and regulators about the board and management's attitude toward the fraud risks. The board of directors, as the representative body of shareholders, sets the general tone for the organization to pursue for the best interests of the shareholders, but delegates the responsibility for designing, operating, implementing internal control to management. The board monitors management's influence over the control environment and assesses the effectiveness of the internal control with the help from the audit committee.

Internal control is a system designed to provide reasonable assurance about safeguarding assets, reliable financial information, compliance with laws and regulations, and efficiency and effectiveness of business operations. The entity's tone at the top based on honesty and integrity provides the foundation upon which internal control system can be operated as designed. In addition, continuous monitoring and implementation of the system, and feedback from internal and external auditors will make the system achieve its objectives.

## REFERENCES


Albrecht, W.S, C. C. Albrecht, C.O. Albrecht, and M .F.Zimmerman(2009), *Fraud Examination* (South-Western Publishing Co.)

American Institute of Certified Public Accountants (1997), *Statement on Auditing Standards No.82 : Consideration of Fraud in a Financial Statement Audit*, New York:AICPA.

Arens, A.A., R.J. Elder, and M.S. Bealey (2008), *Auditing : An Integrated Approach* (Prentice - Hall)

Association of Certified Fraud Examiners(ACFE 2008), *The Report to the Nation on Occupational Fraud and Abuse*, Austin, Tx

Barnett, Andrew H, James E. Brown, Robert Fleming, and William J. Reed ( May, 1998), "The CPA as Fraud - buster," *Journal of Accountancy*, pp.69 - 73.

Barton, M. Frank and Mason L. Rockwell (January, 1991), " Who's Responsible for the Content of Financial Statements?," *Management Accounting*, pp.24 - 26.

Browning, E.S., and I. Dugan (Dec.16, 2002) "Aftermath of a market mania", *Wall Street Journal*

Bull, Ivan, "Board of Director Acceptance of Treadway Responsibilities (February, 1991)," *Journal of Accountancy*, pp.67 - 74.

Bliss, Edwin C. (July 15, 1994), "Employee Thefts," *Boardroom Reports*, pp.5-6

Committee of Sponsoring Organizations of the Treadway Commission (COSO 1999), *Fraudulent Financial Reporting: 1987-1997, An Analysis of U.S. Public Companies*, New York.

Cottrell, David M. and Steven M. Glover (July, 1997), "Finding Auditors Liable for Fraud," *CPA Journal* pp.14 - 21.

Glover, Hubert D. and June Y. Aono (1995), "Changing the Model for Prevention and Detection of Fraud," *Managerial Auditing Journal* pp.3 - 9.

Institute of Internal Auditors (IIA, Nov. 2005) *Tone At the Top*, Almonte Springs, FL

Jensen, M.C., and W.H. Meckling (1976), "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure", *Journal of Financial Economics* pp. 305-360.

Knox, John (February, 1994), "Why Auditors Don't Find Fraud," *Accountancy* p.128.

National Commission On Fraudulent Financial Reporting (1987), *Report of the National Commission on Fraudulent Financial Reporting* [Treadway Report], Washington, D.C.: Government Printing Office.

Pincus, K.V., M. Rusbarsky, and J. Wong (1989), "Voluntary Formation of Corporate Audit committee among NASDAQ Firms," *Journal of Accounting and Public Policy*, pp. 239-265.

Ratcliffe, Thomas A. and Paul Munter (May, 1998), "Application of SAS No.82 to Audits of Small Business," *National Public Accountant*, pp.22-27.

Schneider, Arnold and Neil Wilner (July, 1990), "A Test of Audit Deterrent to Financial Reporting Irregularities Using the Randomized Response Technique," *The Accounting Review*, pp.668-681.

Zimbelman, Mark F (Supplement, 1997), "The Effects of SAS No.82 on Auditors' Attention to Fraud Risk Factors and Audit Planning Decisions," *Journal of Accounting Research* pp.75-98.

www.iht.com/articles/2008/12/21/business/madoff.php

www.washiontonpost.com/wp-dyn/content/article/2009/02/28/AR2009022801905.htm