Iranian Accountants Conception Of The Prevention Methods Of Fraud And Offering Some Recommendations To Reduce Fraud In Iran

Morteza Ramazani[1],Hossien Rafiei Atani[2]

GJMBR Classification
FOR:150199,160504

***Abstract*-The purpose of this study is to examine the extent to which accountants, internal auditors, and certified fraud examiners use fraud prevention and detection methods, and their perceptions regarding the effectiveness of these methods in Iranian companies. Research method has been survey was administered to 178 accountants, internal auditors and certified fraud examiners. Findings of this research results indicate that firewalls, virus and password protection, and internal control review and improvement are quite commonly used to combat fraud. However, discovery sampling, data mining, forensic accountants, and digital analysis software are not often used, despite receiving high ratings of effectiveness. In particular, organizational use of forensic accountants and digital analysis were the least often used of any anti-fraud method but had the highest mean effectiveness ratings. The lack of use of these highly effective methods may be driven by lack of firm resources.**

Keyword-Detection fraud, Accountants Conception, Prevention Fraud Reduce Fraud, Iran

I. INTRODUCTION

Most industrialized countries have experienced a flurry of occupational fraud cases lately, including the Enron, WorldCom, Societe Generale, and the Parmalat frauds, just to name a few. Occupational fraud may be defined as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" (ACFE and Peltier-Rivest, 2007).

Any fraud committed by an employee, a manager or executive, or by the owner of an organization where the victim is the organization itself may be considered "occupational fraud" (sometimes called "internal fraud").

Recent. Recent corporate financial accounting scandals (e.g. Enron, WorldCom, Global Crossing, Tyco, etc.) h concerns about fraud, wiped out billions of dollars of shareholder value, and led to the erosion of investor confidence in financial markets (Peterson and Buckhoff, 2004; Rezaee et al., 2004).One reason that entities of all types are taking more and different steps to fight fraud is that the traditional red flags approach is not considered effective. The well-known red flags approach involves the use of a checklist of fraud indicatorsThe existence of red flags does not portend the presence of fraud but represents conditions associated with fraud; they are cues meant to alert an auditor to the possibility of fraudulent activity (Krambia-Kardis, 2002). Numerous commentators have cast doubt on the red flags approach as it suffers from two limitations:

(1) red flags are associated with fraud, but the association is far from perfect, and

(2) since it focuses attention on specific cues it might inhibit internal and external

auditors from identifying other reasons that fraud could occur (Krambia-Kardis,2002). The new standard continues to require the auditor to plan and perform the audit to provide a reasonable assurance that the financial statements are free of management fraud[1]. SAS No. 110 issued by Auditing Standards Board of the Institute of Chartered Accountants of England and Wales also provides similar standards on fraud detection. Costello (1991) analyses court cases concerning fraud and found that neither the generally accepted auditing standards (GAAS) nor SAS No. 53 constitute the controlling measures of an auditor's liability A second reason that organizations are trying more and different ways to attack fraud is that most entities have used an impractical strategy of fraud detection (Wells, 2004) According to the 1996 Report to the Nation on Occupational Fraud and Abuse (The Wells Report), fraud and abuse cost US organizations more than $400 billion annually (ACFE, 1996). A KPMG Peat Marwick fraud survey of large and mid-size firms found that 62 per cent of those companies had experienced fraud during the past year (KPMG Peat Marwick, 1998). The median loss per fraud incident for firms of all sizes was $117,000 (KPMG Peat Marwick, 1998). One survey by the Association of Certified Fraud Examiners (ACFE, 1996) found that the median loss per fraud incident for companies with fewer than 100 employees was $120,000. Although no industry was immune to fraud losses, those with the largest reported median fraud losses per occurrence are real estate financing, manufacturing, banking, construction, health care, and retail (ACFE, 1996).

In the Fall 1997 issue of the Auditor's Report, the American Accounting Association (AAA) encouraged research directed toward assisting auditors and investigators in preventing and detecting fraud. The growth in fraud cases indicates that a strong need exists for research approaches that better enable auditors and investigators to prevent and detect potential fraud. Thus, the purposes of this study are to

About[1]- University of Applied Sciences and Technology (UAST) Zanjan Branch, Zanjan, Iran
Tell: 98-93-5825-1860E-mail: Mortezaramazani@ymail.com
About[2]- Islamic Azad University (IAU), Zanjan Branch, Sama College, Zanjan, Iran
Tell: 98-93-5886-4878 E-mail: Hrafieiatani@ymail.com

analyze and understand accountants' perceptions of the myriad techniques used to combat fraud, shed light on whether the techniques actually used by firms are considered the most effective and offer suggestions to practitioners as to what prevention and detection techniques are the "best." Organizational management attempting to comply with SOX and similar laws by launching new anti-fraud programs, as well as external and internal auditors, will benefit from this study's findings, when considering which anti-fraud methods to pursue. The benefits consist of less time spent on the use of ineffective techniques and reduction of fraud risk through earlier implementation of more effective fraud prevention and detection techniques.

As we inter new millennium, the recipients of financial statements have become a far sophisticated and informed group. The demand more from an audit function than a mere attestation with regard to auditor responsibility still be account for, furthermore during the last years, there has been a great number of accounting scandals throughout the world; most recent among then are; Enron, WorldCom, Parlmalat, and Famie Mac. These scandals have seriously damaged the confidence in financial reporting, because of fraud. After these huge number of scandals had profound impact on the profession, leading to the disbanding of the Public Oversight Board (Mulligan, 2002) and the collapse of Arthur Andersen, one of the world'' largest accounting firms (Bayer). New legislation (e.g. Sarbanes -–Oxley Act of 2002) and a new oversight board are just a few of the effects of these scandals.

II. Symptoms of Fraud in a Corporate Environment

Existing fraud-detection literature shows that fraud symptoms can be placed into three broad categories: 1) symptoms that relate to the corporate environment of the firm, which include management style, incentive systems, a firm's overall ethics, industry stresses, and a firm's relationships with outside parties; 2) symptoms that relate to the perpetrator, such as any financial or work related pressures, opportunities to commit fraud, and rationalization of the fraud; and 3) symptoms that relate to financial records and accounting practices

.

III. The Cost of Fraud

The US Chamber of Commerce estimates that the annual cost of fraud exceeds $100 billion. This big bill for fraud is not paid by its perpetrators, rather it is paid by innocent parties including consumers, insurance companies and public servants such as external auditors. The cost of fraud eventually bites into the profitability of the victimized organization as well as the stability of the US economy. The impact of fraud can be viewed from both a micro and a macro perspective.(Hubert D. Glover and June Y. Aono, 1995)

IV. Fraud Duty

Fraud involves a misallocation of resources or distorted reporting of the availability of resources. This contradicts the elements of sound and prudent management. Fraud impairs efficiency, productivity and innovation because it siphons away resources to non-constructive activities.

This limits an organization's ability to manage, grow and succeed. For example, the Drexel Burnham Lambert case resulted in the demise of one of Wall Street's most prestigious firms. The glamour associated with Michael Milken, who will undoubtedly survive, is overcast by the thousands of lost jobs. In addition, what about the host of investors who lost their life savings owing to the scandal? Likewise, the MiniScribe case cost jobs as well as the credibility of its auditor Coopers & Lybrand. Corporations cannot remain healthy and remain competitive if fraud continues to go undetected. The resources misallocated threaten the longevity of a firm. Losses incurred owing to fraud can be translated into decreased sales, employment, productivity, and credibility. In fact, the only increase associated with fraud is the cost of legal and insurance protection (Mokhiber, R)

V. Sarbanes-Oxley Act

Following some high-profile cases of fraudulent financial reporting, the SEC (2003) adopted new auditor independence rules. Originating from the belief that substantial revenues from NAS could compromise auditors' objectivity, these rules prohibit accounting firms from providing, together with the audit of a public client, certain NAS. While SOX allows the provision of tax services to an audit client by the same firm, the SEC Adopting Release (SEC, 2003) cautioned audit committees to be careful that such services do not impair independence. In fact, the significant concern about auditors' objectivity prompted the U.S. Senate Banking Committee to examine the need for barring certain additional services provided by external auditors, including tax services, to the public companies they audit (U.S. Senate Committee on Banking, Housing, and Urban Affairs, 2003). At the same time, the Conference Board's Commission on Public Trust and Private Enterprises released its 2003 best practice suggestions, which recommend that accounting firms limit themselves to audit and closely related services. While Kinney et al. (2004) provided an interesting empirical linkage between the provision of tax services and public company restatements, there is still no evidence as to whether the provision of tax services to non-public audit clients affects auditors' objectivity. Several factors drive the need to examine this segment of the audit market. While SOX rules apply only to public registrants, the AICPA (2002) is concerned that SOX concepts may cascade to the state level and the audits of non-public companies most often audited by small- and medium-sized firms. Substantial limitations on tax services, offered by accountants to privately owned audit clients, could have serious economic effects on small businesses and accounting firms. Some have argued that limiting an auditor's ability to provide tax services to audit

clients would result in less independent review of tax strategies and less transparency for investors (Ernst & Young, 2003). Auditors today are much more tax focused than in the past, since many firms provide tax awareness programs that alert auditors to instances when clients can benefit from adopting new tax strategies (Temple, 1992). For example, during the auditor's review of the organizational structure and related parties, the auditor might consider the possibility of merging multiple C corporations into one S corporation, adopting an employee stock ownership plan (ESOP), which offers numerous financial and tax advantages, or reconsidering the client's plans for succession and related estate and gift tax concerns.

According to the Small Business Administration (2003), over 99% of accounting firms qualify as small businesses with less than $3 million in revenues and the great majority of all accounting firms consist of one office. Because auditors in small- and medium-sized firms often assist in tax work, study of auditors' objectivity in this segment of the audit market is important. For example, auditors in small- and medium-sized firms often use tax accrual checklists – a reminder list for auditors to see that the tax consequences of potentially significant events have been considered by the client in making the income tax accrual – and tax-savings checklists an idea triggering device to identify tax planning and saving matter for clients (Primoff, 1992). Hence, this study specifically focused on the provision of tax services to non-public companies by small- and medium-sized firms.

VI. Reasons for Committing Fraud

The respondents suggested the following factors from their experience as the reasons for committing fraud (Philmore Alleyne, Philmore Alleyne):

- . the moral values of individuals;
- . the need to maintain an increasing social status;
- . persons unhappy with their job;
- . persons with drugs and gambling addictions;
- . people with increasing indebtedness;
- . individuals who "see other people doing it"; and
- . persons who feel that they would not be caught.

The understanding and reaction to fraud was determined not only by the size of the fraud and who committed it, but also against which organization the fraud was committed. One manager from a financial institution said that:

Organizations like financial institutions keep such matters in-house and try to recover losses or minimize erosion of public confidence by not prosecuting perpetrators of fraud. Banks, credit unions and insurance companies are organizations most likely to have fraudulent activity.

VII. Analytical Procedures as a Method of Fraud Detection

In 1987, the Treadway Commission reported, "The potential of analytical review procedures for detecting fraudulent financial reporting has not been realized fully (National Commission on Fraudulent Financial Reporting [NCFFR], 1987)." Based upon a review of actual fraud cases, the Treadway Commission observed that financial statement frauds tend to be very similar in terms of how they are perpetrated. Most fraudulent cases involve improper revenue recognition, overstatement of assets, and/or improper deferral of expenses. Typically, analytical procedures involve comparing actual financial statement amounts with expected amounts that are derived from the application of a naive or complex prediction model. Since the misstatements resulting from fraudulent misrepresentations result in differences from predicted amounts, they should be potentially detectable with analytical procedures. The central task of an auditor in applying analytical procedures is to develop expectations. The expectations the auditor develops will be based upon both the external information that the auditor encounters and his/her own existing knowledge stored in memory. An auditor's existing knowledge is an important factor in his/her understanding and interpretation of information, and can be expected to influence the auditor's effectiveness in assessing the risk of financial statement fraud. Research on experience and expertise suggests that an individual's knowledge changes as experience increases (Chi, Glaser & Rees, 1982), thus an auditor's performance of analytical procedures may be affected by experience. Previous research in both psychology and auditing has found that as individuals gain relevant experience their knowledge structures change and develop (Chi et al., 1982). Generally the findings indicate that experienced individuals have greater total knowledge (Christ, 1993; Knapp, 1995; Libby & Frederick, 1990; Tubbs, 1992), more understanding of relationships between variables (Chi et al., 1982; Frederick, 1991; Moeckel, 1990), and an ability to go beyond the surface features of information and identify the true, underlying problem (Biggs, Mock & Watkins, 1988; Chi et al., 1982; Christ, 1993; Moeckel, 1990). All of these characteristics of knowledge are potentially important to the task of fraud risk assessment with analytical procedures. Two empirical studies of particular importance to the issues addressed here have both found significant knowledge differences between audit managers and seniors. Christ (1993) studied auditors' planning knowledge (of which preliminary analytical procedures are a subtask) with a recall task. She found significant differences in the knowledge structures of audit managers/partners as compared to senior and junior auditors. Knapp (1995) examined auditors' knowledge of factors that may indicate the existence of financial statement fraud and found significant differences. Managers were able to recall a greater number of ``factors that may suggest the existence of fraud in a set of financial statements'' than were audit seniors. Given that significant knowledge differences have been identified between experience levels of auditors, this knowledge difference will likely affect auditors' understanding and interpretation of information during analytical procedures and, thus, their ability to effectively assess the risk of financial statement fraud.

VIII. Role of Internal Auditors in Detecting Fraud

There is considerable evidence that fraud is a serious problem and fraud detection is inadequate. The Association of Certified Fraud Examiners (ACFE) issued a report

indicating that fraud has cost U.S. firms over $600 billion annually (ACFE, 2002). A 2003 KPMG Peat Marwick survey reported that 75% of the surveyed firms had experienced fraud in the last year, with an average loss of $296 million, up from an average of 62% experiencing fraud with an average loss of $117 million in 1998. Fraud detection has also been inadequate, as evidenced by recent, very public audit failures. The ACFE Report to the Nation (ACFE 2002) noted that external auditors detected only 11.5% of the frauds reported, while internal auditors detected 18.6%.1 As the internal defenders of a firm's longevity, internal auditors are "obligated to be alert to the signs and possibilities of fraud" (Hillison et al. 1999, 351). While external auditors focus on misstatements in the financial statements that are material in scope, internal auditors are often in a better position to detect the symptoms that accompany asset theft, as well as financial statement fraud (See SAS 99 2002). Unlike external auditors, internal auditors have a continual presence in the company that provides them with better understanding of the organization and its control system (Perry et al. 1997)2. Thus, internal auditors are in a position to take on the elevated role established by the Sarbanes Oxley Act to assist external auditors in their search for internal irregularities (Leibs 2004). In addition, their internal presence should assist in establishing fraud prevention measures (Hillison et al. 1999). The Standards for the Professional Practice of Internal Auditing (IIA Standards) requires internal auditors to assess risks faced by their organizations and develop audit plans and internal controls testing accordingly. SAS 99 expands on this role by encouraging internal auditors to "conduct proactive audits to search for corruption, misappropriation of assets, and financial statement fraud." Internal auditors should be expected to assist in the prevention and identification of fraud signals and weaknesses in the control system (Ratliff et al. 1996). Perry et al. (1997, 42) encourage organizations to "heighten the responsibilities of the internal auditor to include the duties of both 'monitor' and 'investigator' so that the organization can be better protected from internal fraud."

IX. Audit Committee Quality and Internal Control

Since an entity's internal control is under the purview of its audit committee (Krishnan, 2005), we investigate the relation between audit committee quality and internal control weaknesses. The audit committee not only plays an important monitoring role to assure the quality of financial reporting and corporate accountability (Carcello and Neal, 2000), but also serves as an important governance mechanism, because the potential litigation risk and reputation impairment faced by audit committee members ensure that these audit committee members discharge their responsibilities effectively. We thus expect that firms with high-quality audit committees are less likely to have internal control weaknesses than firms with low-quality audit committees.

On measuring audit committee quality, we focus on the financial expertise in these committees. The Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (BRC)'s (1999) recommendation that each audit committee should have at least one financial expert highlights the importance of the financial literacy and expertise of audit committee members.5 Section 407 of the SOX incorporates the above suggestion and requires firms to disclose in periodic reports, whether a financial expert serves on a firm's audit committee and, if not, why not. Such financial expertise of audit committee members has been shown to be important for dealing with the complexities of financial reporting (Kalbers and Fogarty, 1993) and for reducing the occurrence of financial restatements (Abbott et al., 2004). In addition, DeZoort and Salterio (2001) find that audit committee members with financial reporting and auditing knowledge are more likely to understand auditor judgments and support the auditor in auditor-management disputes than members without such knowledge. Moreover, financially knowledgeable members are more likely to address and detect material misstatements. Audit committee members with financial expertise can also perform their oversight roles in the financial reporting process more effectively, such as detecting material misstatements (Scarbrough et al., 1998; Raghunandan et al., 2001). Indeed, Abbott et al. (2004) find a significantly negative association between an audit committee having at least one member with financial expertise and the incidence of financial restatement. Krishnan (2005) presents evidence that audit committees with financial expertise are less likely to be associated with the incidence of internal control problems. Therefore, we have the following directional prediction.

X. Public Policy and Authoritative Standards

Over a decade ago, the General Accounting Office (GAO, 1989) noted that economic and political factors led to many financial institution failures in the 1980s. The GAO also found that adherence to sound internal controls, effective management practices and solid financial reporting are essential to ensuring the banking system's safety and soundness. However, bank management often failed to implement adequate internal controls to ensure safe and sound bank operations or compliance with laws and regulations. Recognizing the increased risk of fraud and misstatement in financial reporting should affect public policy and regulation decisions, including the issuance of authoritative accounting and auditing pronouncements. Historically, lending has provided the single largest source of bank earnings and accounted for the largest category of assets. Of the banks that failed in 1987, 79% had not implemented adequate and prudent general procedures to guide loan department personnel in the loan underwriting and approval process. Poor loan documentation was cited in 41% of 1987 bank failures, a period in which banks often failed to obtain such documentation as current statements of cash flows, business plans, building inspections, appraisals and Uniform Commercial Code filings. The Tax Reform Act of 1986 contributed greatly to the collapse of many S&L institutions that had invested heavily in real estate and mortgages (Cordato, 1991). As the market value of real

property decreased due to the Tax Reform Act, so did the value of the S&Ls' major assets, leaving some institutions with negative capital balances.

In 1987, the Treadway Commission stated that "regulatory and law enforcement agencies provide the deterrence that is critical to reducing the incidence of fraudulent financial reporting." The SEC's financial fraud enforcement program already has raised corporate and public accounting's awareness of the problem and potential for detection and punishment, demanding that management and the public accounting profession reduce intentional misstatements in financial statements. For public accountants, punishment has mostly led to CPA resignations from practice, and other sanctions and censures (Kunitake, 1987). The SEC has taken similar action against key corporate executives. More recently, the popular press has followed management fraud cases such as Enron and WorldCom that should lead to executive jail time. However, further improvements can and should be made at both the state and federal levels.

In 1987, the Treadway Commission stated that "regulatory and law enforcement agencies provide the deterrence that is critical to reducing the incidence of fraudulent financial reporting." The SEC's financial fraud enforcement program already has raised corporate and public accounting's awareness of the problem and potential for detection and punishment, demanding that management and the public accounting profession reduce intentional misstatements in financial statements. For public accountants, punishment has mostly led to CPA resignations from practice, and other sanctions and censures (Kunitake, 1987). The SEC has taken similar action against key corporate executives. More recently, the popular press has followed management fraud cases such as Enron and WorldCom that should lead to executive jail time. However, further improvements can and should be made at both the state and federal levels.

In response to public demand for more reliable financial information, the SOA Act contains many provisions that greatly affect auditor responsibilities, including stricter independence guidelines, increased financial statement disclosures and greater corporate responsibility (e.g. CEOs and CFOs also "signing off" on financial statements). Such large-scale debacles at public companies as Enron and WorldCom also raised the question of whether greater government regulation of accounting rules should exist. In an apparent step in that direction, the Public Company Accounting Oversight Board (PCAOB), an organization deriving its power from the SOA, establishes rules relating to the preparation of audit reports for issuers. Subject to SEC oversight, the PCAOB conducts inspections, investigations, and disciplinary proceedings with accounting firms who audit
public companies.

SAS No. 53 (AICPA, 1998), through using the term "irregularities," offered guidance on an auditor's responsibility to plan audits to search for financial statement fraud. A decade later, SAS No. 82 (AICPA, 1997) required auditors to identify the presence of risk factors, primarily by assessing the risk of fraudulent material misstatement in each audit. Crucial to the risk assessment is a bank's move towards an increasingly risky asset/investment mix. In 1988, the SEC also issued Financial Reporting Release (FRR) No. 28, containing industry-specific disclosure guidance for loan losses to help determine allowances for loan losses for registrants engaged in lending activities. The issuance of the Treadway Commission's Report, SAS No. 53 and FRR No. 28 all illustrate increased public attention to bank fraud. Moreover, SAS No. 99, effective in 2003, builds upon SAS No. 82 to expand auditor guidance for detecting material fraud in financial statements. While not technically changing auditors' responsibilities, SAS No. 99 encourages increased *professional* skepticism (an objective, questioning mindset) in all audits and requires "brain-storming" among engagement team members to identify potential fraud risk areas before and during the audit.

The Committee of Sponsoring Organizations of the Treadway Commission (1999) noted that between 1987 and 1997, about half of the firms that committed financial statement fraud recorded revenues prematurely or created fictitious revenue transactions. One-half that recorded fictitious assets should have expensed. Auditors should understand that audit procedures designed to address an increased risk in errors could respond ineffectively to increased risks of fraud (Bloomfield, 1995). Management can alter existing information, withhold data or use other methods to avoid detection from auditors who use common error detection methods in performing their duties. For example, Erickson et al. (2000) reviewed the CPAs' working papers in the Lincoln S&L fraud found that: (1) while following the dictates of SAS No. 82 would have detected some fraud issues, still more guidance is needed; and (2) increasing traditional audit procedures would not have cast doubt or suspicion on Lincoln S&L's questionable revenue recognition procedures. Adapting audit plans to accommodate changing levels of fraud risk allows auditors to improve their ability to detect financial statement fraud.

XI. Methods of Prevention Fraud

Both fraudulent financial reporting and asset misappropriation have become major costs for many organizations. Numerous fraud prevention and detection techniques are now utilized to reduce the direct and indirect costs associated with all forms of fraud. These various techniques include but are not limited to: fraud policies, telephone hot lines, employee reference checks, fraud vulnerability reviews, vendor contract reviews and sanctions, analytical reviews (financial ratio analysis), password protection, firewalls, digital analysis and other forms of software technology, and discovery sampling (Carpenter and Mahoney, 2001; Thomas and Gibson, 2003). Organizations that have not been fraud victims tend to rely more on intangible prevention tools such as codes of conduct or fraud reporting policies while those that have suffered fraud have implemented more tangible measures such as whistle-blowing policies and fraud prevention and detection training (PriceWaterhouseCoopers (PWC), 2003).

A. Maintain a fraud policy

Every organization should create and maintain a fraud policy for guiding employees. A corporate fraud policy should be separate and distinct from a corporate code of conduct or ethics policy. A model or sample fraud policy is available from the ACFE. Such a fraud policy should be clearly communicated to employees. Various avenues of communication include use in orientation of new hires, employee training seminars, and annual performance evaluations. Written acknowledgment by each employee that the policy has been read and understood should be required.(James L. Bierstaker, Richard G. Brody, Carl Pacini,2006)

B. Establish a telephone hotline

A rather novel fraud approach that is becoming more common is the use of anonymous telephone hotlines (Holtfreter, 2004). It is a very cost effective means for detecting occupational fraud and abuse. A hotline allows employees to provide confidential, inside information without the fear of reprisal that accompanies being a whistleblower (Pergola and Sprung, 2005).

Hotlines may be supported in-house or provided by a third party. An example of a third-party hotline is a subscription service offered by the ACFE. The annual subscription rate may be quite modest. The results of all calls are provided to the client within two or three days. A hotline is not only an effective detection tool but it also enhances deterrence. Potential perpetrators will likely have second thoughts when considering the risks of being caught.

C. Employee reference checks

Organizations should conduct employee reference checks prior to employment. An employee with a history of perpetration of fraud schemes may move from one organization to another. When employee references are not checked, a dishonest person may be hired. A dishonest employee can defraud an unsuspecting organization of thousands of dollars and move on to a new job before the fraud is discovered. Resumes should be scrutinized and information verified to determine that the information provided is legitimate. An organization should not rely on the telephone numbers listed on the resume for prior employers, as they may be false. Employer phone numbers should be obtained by the organization independently.

Organizations should conduct a second reference check six months after an employee starts work. The reason for a dishonest employee's recent dismissal from a previous job may not have had time to become part of the employee's record during the initial search. This may be discovered by a second check..(James L. Bierstaker, Richard G. Brody, Carl Pacini,2006)

D. Fraud vulnerability reviews

A fraud vulnerability review that investigates the organization's exposure to fraud should be performed. This includes an assessment of what assets are held and how they could be misappropriated. For those organizations involved in electronic commerce, a vulnerability review should also include an assessment of exposure to employee misappropriation or destruction of such "non-balance" sheet items as confidential customer data and financial information. The purpose of such a review is to "outsmart the crooks." A vulnerability review can help to direct an internal audit plan and, in particular, to highlight the most vulnerable assets. The review is considered a proactive step in fraud prevention and detection. Consideration of each class of asset and the evaluation of the exposure to loss helps the auditor or accountant to see what the thief sees. Steps then should be taken to eliminate, minimize, or at least control the exposures..(James L. Bierstaker, Richard G. Brody, Carl Pacini,2006)

E. Perform vendor contract reviews

Review of company contracts and agreements can provide an indication of possible contract fraud, including kickbacks, bribery, or conflicts of interest by an organization's employees. Contract fraud can occur when a trade supplier fraudulently takes advantage of a contract to make illegal profits. Contract fraud may involve a conspiracy between entity personnel and a trade supplier or conspiracy among two or more vendors.

Analyzing contract files for the same contractor routinely bidding last, bidding lowest, or obtaining the contract may detect this type of contract fraud. Awarded contracts may also be scrutinized for evidence of a supplier regularly being awarded contracts without indication of a legitimate reason for the constant receipt of contract awards. Such a review may reveal that bribes or kickbacks are the reason for the awards. A review of various public records may reveal whether an employee has a covert ownership interest in the contractor. .(James L. Bierstaker, Richard G. Brody, Carl Pacini,2006)

F. Use analytical review

Fraud can affect financial statement trends and ratios. Accounts that are manipulated to conceal a fraud may manifest unusual relationships with other accounts that are not manipulated. Also, erratic patterns in periodic account balances may occur because the fraudster may engage only sporadically in fraudulent activity. Financial analysis conducted by an accountant or investigator may reveal existing relationships that are not expected or the absence of relationships that are expected to be present.

It may behoove the accountant or investigator to analyze several years of financial statement data using different techniques to obtain a clear picture of the financial impact of any fraud scheme. Various analytical review techniques which the accountant or investigator may employ include: trend (horizontal) analysis, ratio analysis (vertical analysis or common size statements), budgetary comparisons, comparisons with industry averages, and review of general ledger and journal entries. Unusual items should be pursued to determine if fraud could be the cause of an aberration..(James L. Bierstaker, et al,2006)

G. Password protection

The growth of the internet and e-commerce has led to a rise in the number of dial-in ports to computer networks thus increasing the exposure to fraud. Accountants and investigators should assure that only legitimate users have access to the computer network and associated data. Although passwords are the oldest line of computer defense, they still constitute the most effective and efficient method of controlling access.

The difficulty with passwords is that there is an inverse relationship between making the password effective and usable. If password requirements are too complex, users will write the password down, placing it at risk (Gerard et al., 2004). Therefore, every organization needs to evaluate the tradeoffs. Passwords should be six to eight characters long with a mix of letters, numbers and special symbols. Users should be required to change their password often, for example, every 30-60 days. Additionally, users should have to cycle through 6-12 different passwords before being allowed to reuse a password (Gerard et al., 2004). Also, employees should not be allowed to display their passwords in any location where unauthorized individuals may see them. Lockout procedures should be implemented if a user fails to input a correct password after three attempts.

Technology has advanced to create new forms of password protection using biological features of the user (i.e. biometrics) such as voiceprints, fingerprints, retina patterns, and digital signatures. New forms of password protection are likely to become cost effective in the near future.

H. Firewall protection

One necessary technique for controlling unauthorized access is the use of firewalls. Firewalls can be used at the software or hardware level. At the software level, there are specific programs (e.g. ZoneAlarm from zonelabs.com) that can be coordinated with internet-related software programs (browsers, e-mail, etc.) to protect the data being passed through them. Hardware firewalls/routers basically prevent people from finding an organization's connection to the internet. The internet connection is known as an IP address. The hardware firewall/router basically hides the IP address so that hackers cannot find and access it (Gerard et al., 2004).

I. Digital analysis

Digital analysis, which is based on Benford's Law, tests for fraudulent transactions based on whether digits appear in certain places in numbers in the expected proportion. A significant deviation from expectations occurs usually under two conditions. The first condition is that a person has added observations on a basis that does not conform to a benford distribution. The second condition is that someone has deleted observations from a data set that does not adhere to a benford distribution (Durtschi et al., 2004).

Tax cheats, check forgers, and embezzlers simply cannot consciously generate random numbers. Forensic accountants and auditors have depended on this human quirk for years and various types of digital analysis software, including DATAS, have proven themselves capable of pinpointing this habit (Lanza, 2000). A list of examples of data sets where digital analysis software may be used includes investment sales/purchases, check registers, sales and price histories, 401 (k) contributions, inventory unit costs, expense accounts, wire transfer information, life insurance policy values, bad debt expenses, and asset/liability accounts.

Other types of fraud exist that cannot be detected by digital analysis because the data sets under examination are not appropriate for such analysis. For example, duplicate addresses or bank accounts cannot be uncovered, yet two employees with similar addresses might signal a shell company. Digital analysis will not detect such frauds as contract rigging, defective deliveries, or defective shipments.

J. Discovery sampling

Discovery sampling is a form of attribute sampling. The latter is a statistical means of estimating the percentage of a population that possesses a particular characteristic or attribute. Discovery sampling is based on an expected error rate of zero. It is employed when the accountant needs to know whether a population contains any error indicative of fraud. If a single case of significant error or fraud is found in a sample, the sampling process is stopped and the error or fraud is investigated.

Let us consider an example. An account should not include any payments made out to a vendor name that is known to be fictitious unless there is that type of fraud in the account. If there is no such fraud in the account, there should be no payments to fictitious vendors. If an auditor were to test some of the payments in an account and were to find a payment made out to a fictitious vendor, the auditors would know that fraud existed but would not know the extent of the fraud. Conversely, if an accountant examined some account payments and did not find any illegitimate payments, he or she would not conclude that no fictitious payments existed in the account. .(James L. Bierstaker, et al,2006)

XII. DETECT MANAGEMENT FRAUD

The responsibility of the independent auditor to detect management fraud remains a controversial issue. American Institute of Certified Public Accountants recently issued a new Statement on Auditing Standard entitled Consideration of Fraud in a Financial Statement (AICPA, 1997) which supercedes SAS No. 53 (AICPA, 1988).

The new standard continues to require the auditor to plan and perform the audit to provide a reasonable assurance that the financial statements are free of management fraud .

Management fraud is also associated with explosion of litigation against the auditor (Palmrose, 1991).

Auditing can detect management fraud, but audit procedures are not designed to guarantee that the financial statements are free from management fraud. Arens and Loebbecke (1997) contend that management fraud is inherently difficult to uncover because management is in position to override internal controls and can actively conceal the misstatements

XIII. A Theory of Successful Fraud Detection

To explain successful fraud detection we propose that auditors apply the same intentional stance strategy that deceivers use, as we described above. Just as the deceiver solves the problem of creating a deception by using knowledge of how the victim thinks and acts, the detector needs to solve the inverse problem of detecting the deception that has been created by using knowledge of how the deceiver thinks and acts (Wilks and Zimbelman 2004). We assume that both deceiving and detecting deception are accomplished by thinking about the other agent goals, knowledge, and possible actions, i.e. by adopting the intentional stance. The deceiver uses the intentional stance to manipulate information cues and mislead its intended victim. The detector use the intentional stance to "reverse engineer" the cues left behind by the deceiver and identify them as symptoms of attempts to mislead. Just as the six *deception* tactics described above express the deceiver's knowledge, we conjecture that detectors learn corresponding *detection* tactics to counter what the deceiver has attempted to do. For example, the masking tactic is countered by a corresponding anti-masking tactic, which consists of realizing that something (e.g., an expense or a liability) appears to be missing because it has been intentionally concealed by the deceiver. Knowledge of the detection tactics comes from experience. Not necessarily from specific experience with fraud per se, which is scant, but from experience with deception in general, which is more abundant. Auditors, as any other social agent, have frequent and varied exposure to instances of deception, both as a deceiver and/or victim or intended victim of deception (e.g., Ekman 1992; Ceci , Leichtman, and Putnick 1992). As a way to cope with potentially deceiving adversaries, social agents develop knowledge for detecting the deceptions created by others (Vasek 1986). This general detection knowledge is specific to the task of detecting deceptions, but is not expressed in terms of domain content (Cosmides 1989; Cosmides and Tooby 1992). In the specific case of fraud detection, auditors interpret cues found in financial statements in the light of goals ascribed to management, as well as tactics they believe management may potentially have used to manipulate the information are attempting to evaluate. The detection tactics are heuristics that are activated in the presence of three conditions: 1) the discovery of an anomaly, 2) the belief that the anomaly is functional to the goal ascribed to the potential deceiver (e.g., management) and 3(the belief that the anomaly could be the result of the deceiver's intentional manipulation. For example, the conditions for applying an anti-masking tactic are that the auditor 1) notices that something (e.g., an expense or a liability) is unexpectedly missing, 2) concludes that this absence contributes to the goals that have been ascribed to management, and 3) believes that management has the capability of manipulating the reporting process so that the expense (liability) does not get recorded. When these conditions are met, the auditor hypothesizes that the deceiver has masked the unexpectedly missing item and takes corrective action (e.g., searches for evidence, or assumes that the item was maliciously removed).

To be useful, the detection tactics must be applied to specific situations. To continue the above example, in an auditing context a detector must develop expectations about the value of expenditures, she must be able to ascribe goals to management, and whether management could manipulate the accounting process so as to fail to record the expense or liability in the financial statements (e.g., Albrecht, Leichtman, and Putnick 1995). These abilities are enabled by a type of knowledge that we have called mediating knowledge of auditing. Mediating knowledge maps the general conditions of the tactics into entities and relationships in a particular situation. We claim (below) that this mediating knowledge is also the source of errors and thus ultimately the failure to detect deception. The rationale for this claim is that the detection tactics are likely to be quite refined, because of the repeated exposure that individuals have with deception in the world, both as a deceiver and as a target. By contrast, the knowledge necessary to connect a specific situation to a tactic is more likely to be lacking, because in most specific domains the experience of a deception is relatively rare. To summarize, the theory we have proposed describes a solution to the problem of detecting fraud as faced by auditors. It is viable because it satisfies the three general characteristics of the fraud detection problem that were identified at the beginning of this paper. First, it addresses low base-rate, because it argues that this knowledge develops by abstraction from numerous instances of deception to which the auditor has been exposed in everyday life. Second and third, it not only appreciates but also exploits the adversarial and intentional nature of the deceptions created by management as it uses the goals and actions ascribed to management as a basis for detecting the deception they have created. To demonstrate that the theory works we next analyze in detail a computer model that applies the detection tactics to a set of real financial statements, and we run the model on the cases listed in Table 2. The model is described next.

XIV. The Development of Accounting Fraud Recognition Technology

a. *The Quantitative Technologies of Discerning Accounting Fraud*

We can set up linear and non-linear models by studying different data reports, and then make some combinations of these discerning models, which will offer us a better way to solve this problem for most of cases. This is because it is infeasible to discern complicated accounting fraud by only using one single model if we count reliability and risk in. What's more, every kind of model will include some useful independent information; hence we can't fully tap out all the valuable economic information if we only use one single model. The composite discerning model is designed to solve these limits. This model will combine all the other discerning results, thus establish itself as the best discerning method.Research indicates that the connection between financial index and the existence of fraud is universal, thus the exceptional change of financial numerical index can

often expose its tactics. As a result, if we pay more attention to financial index, which reflects the profits, we can discern the means of making frauds to a great extent. Therefore, it is our duty to structure a strong index system where we can detect the frauds by normative research, demonstrations, nerve network and fuzzy methods

b. Characteristic Signals of Accounting Fraud

Regulations, we will face numerous uncertain factors. While auditing the accounting files, we need to adopt diversified testing methods in order to test the existence of accounting fraud from different aspects. Nowadays, the research on discerning accounting fraud in china still remains its elementary level with theoretical analysis and preparation in its early period. Although theoretical circle and economic experts are working hard on it, they haven't established a complete theory and an applied system.Discerning accounting fraud is a kind of complicated and comprehensive management activity where the theory and applications will involve many kinds of disciplines, such as natural science, social science, engineering, systematic science, management science and so on. This paper argues that we can combine different kinds of technologies, such as finance, information technology, controlling and simulation technology into one new applied technology. Upon many case-studies and comparisons, mathematic statistics and model proof, we are determined to design a fraud-recognition system, through which we can calculate and evaluate the data, set up standards for controlling and making decisions. The process of the accounting fraud recognition system. In order to meet the functional demands, we will divide this recognition system into five parts: objective, evaluation and analysis, detective signal and discerning, mid-process control and regulative conduct. Monitoring and predicting the accounting information is developed on the basis of middle control objective. Particularly, we first choose some variables related with accounting fraud, change these variables into mid-objectives after numerical processing; then according to the safe value, we will set up the default value for our case, hence getting the critical values at different significant levels. After setting up the regeneration index system, the corresponding dynamic monitoring system will start to work. This dynamic monitoring system will trace those variables, and make predictions according to the critical values at different significant levels. Also this system will makeadjustments upon the feedback information to correct the unreasonable critical values. In this way, the system of monitoring and discerning accounting fraud is a both stationary and dynamic effective system and the discerning function realizes through above-mentioned risk monitoring, adjusting to the feedback and getting the best results.

XV. Literature Review

Much prior research addressing fraud prevention and detection methods has addressed "red flags." For example, Albrecht and Romney (1986) found in a survey of practicing auditors that 31 flags related to internal control were considered better predictors of fraud. The survey contained a list of 87 red flags. Loebbecke and Willingham (1988) offered a model that considers the probability of material financial statement misstatement due to fraud as a function of three factors:

(1) the degree to which those in authority in an entity have reason to commit management fraud;

(2) the degree to which conditions allow management fraud to be committed; and

(3) the extent to which those in authority have an attitude or set of ethical values that would facilitate their commission of fraud.

Apostolou et al. (2001) surveyed 140 internal and external auditors on the fraud risk factors contained in SAS 82. They document management characteristics as the most significant predictor of fraud followed by client operating/financial stability features, and industry conditions. Chen and Sennetti (2005) apply a limited, industry-specific strategic systems auditing lens and a logistic regression model to a matched sample of 52 computer firms accused of fraudulent financial reporting by the SEC. The model achieved an overall prediction rate of 91 percent for fraud and non-fraud firms.Moyes and Baker (2003) conducted a survey of practicing auditors concerning the fraud detection effectiveness of 218 standard audit procedures. Results indicate that 56 out of 218 procedures were considered more effective in detecting fraud. In general, the most effective procedures were those yielding evidence about the existence and/or the strength of internal controls.

XVI. Research Objectives

This study investigates to measure Iranian accountant conception of fraud and provide policies to prevent it searches for a relationship between the conception of fraud and its reduction.

To measure the level of Iranian accountants awareness of fraud and its prevention methods.

To measure the level of Iranian accountant awareness of Iranian accountants awareness of computer fraud and its prevention methods.

To present suggestions on order to increase awareness of fraud prevention methods.

To provide some plans in order to decrease fraud in Iran.

XVII. Research Methodology

The research methodology used in this study is based on both survey and description methods. So far accurate answer to the research questions, the authors design and developed a questionnaire which it is the most suitable for this study. A survey questionnaire was completed by the accountants of Iranian Company at the end of 2010. The questionnaire contains four parts namely (A) General information and (B). Including elements in fraud prevention methods,(C). elements in computer fraud prevention,(D). questions in reviewing plans to decrease fraud in Iran.

XVIII. THE RESEARCH HYPOTHESES

According to the research problems and objective as well, the following hypotheses were postulated in the study
Iranian accountants are aware of fraud and its prevention methods.
Iranian accountants have enough knowledge about computer fraud and its prevention method.
Some plans have been provided to decrease fraud in iran.
23 independent elements of fraud prevention methods, have same important from the view point of their effectiveness .
7 independent elements of the computer fraud prevention methods have same importance from the view point of their effectiveness.
A survey questionnaire has been provided in these five hypotheses to achieve the aims of this study.

XIX. TESTING OF THE HYPOTHESES

a) *First hypotheses test*

H0: Iranian accountants have no awareness of fraud and its prevention methods.
H1: Iranian accountants have enough awareness of fraud and its prevention methods.
As shown in table (1), t – test value, is 1.521, df is 177, p-value is 0.130, since p-value > 5%, then H0 is accept in. assurance distance of 95%.

b) *Second hypotheses test*

H0: Iranian accountants have no awareness of computer fraud and fraud prevention.
H1: Iranian accountants have enough awareness of computer fraud and fraud prevention.
As shown in table (1), t – test value, is 1.211, df is 177, p-value is 0.228, since p-value > 5%, then H0 is reject in. assurance distance of 95%.

c) *third hypotheses test*

H0: There is some policies to reduce fraud in iran.
H1: There is no policies to reduce fraud in iran.
As shown in table (1), t – test value, is -0.298, df is 177, p-value is 0.766 since p-value > 5%, then H0 is reject in. assurance distance of 95%.

Table (1)

Description Hypotheses	t	df	P-value	**Result**
First hypotheses	1.152	177	0.130	**Accept**
Second hypotheses	1.211	177	0.228	**Reject**
Third hypotheses	-0.298	177	0.766	**Reject**

d) *Forth hypotheses test:*

We have use Friedman's test to prioritize and define the importance of each element to prevent fraud. This test is used when we have statistical data in ordinal type or when we classify them based on ordinal conception. This test shows that if there is most same importance.H0: 23 independent elements to prevent fraud have the same importance from the view points of their effectiveness.H1: 23 independent elements to prevent fraud have not the same importance from the view points of their effectiveness

Table (2-1)

N	**178**
Chi-Square	**453.408**
d.f	**22**
P-value	**0.000**

As shown in table 2-1, p-value = 0 , then H0 is reject in the level of 5% but H1 is accept. In table 2-2, the arrangement order moves from more important to less one.

Table (2-2) independent variables prioritization from the view point of their importance base on Friedman's test

Rank	Independent Variables	**Mean Rank**
1	Bank reconciliations	**16.08**
2	Ethics training	**15.2**
3	Employee counseling programs	**14.02**
4	Security department	**13.44**
5	Increased attention of senior management	**13.25**
6	Operational audits	**13.18**
7	Inventory observation	**13.12**
8	Fraud prevention and detection training	**13.04**
9	Organizational use of forensic accountants	**12.99**
10	Employment control	**12.56**
11	Corporate code of conduct/ethics policy	**12.52**
12	Internal control review	**12.35**
13	Increased role of audit committee	**12.33**
14	Make Detection fraud policy	**12.32**
15	Cash reviews	**12.13**
16	Fraud auditing	**11.93**
17	Fraud reporting policy	**11.69**
18	Make recycle employment policy	**10.09**
19	Make fraud	**9.54**
20	Employment contracts	**9.09**
21	Fraud vulnerability reviews	**9.08**
22	Surveillance of electronic correspondence	**8.27**
23	Code of sanctions against suppliers/contractors	**7.8**

e) Fifth Hypotheses Test

We have use Friedman's test to prioritize and define the importance of each element to prevent computer fraud. This

test is used when we have statistical data in ordinal type or when we classify them based on ordinal conception. This test shows that if there is most importance one among elements or not and if they have same importance in the process.

H0: 7 independent elements to prevent computer fraud have the same importance from the view points of their effectiveness.

H1: 7 independent elements to prevent computer fraud have not the same importance from the view points of their effectiveness

Table (3-1)	
178	**N**
338.600	**Chi-Square**
6	**d.f**
0.000	**P-value**

As shown in table 3-1, p-value = 0 , then H0 is reject in the level of 5% but H1 is accept. In table 3-2, the arrangement order moves from more important to less one.

Table (3-2) independent variables prioritization from the view point of their importance base on Friedman's test

Rank	Independent Variables	**Mean Rank**
1	Virus protection	**5.86**
2	Firewalls	**4.59**
3	Filtering software	**4.46**
4	Digital analysis	**4.15**
5	Discovery sampling	**3.13**
6	Virus protection	**3.01**
7	Data mining	**2.79**

XX. CONCLUSION

To introduce improvements in financial and accountancy methods by processing the procedure of performance stages.Informing process of employees' duties and services to achieve common goals.The reinforcement and organizing authority limitations of audit committee and try to increase them.The reinforcement of relation between members of audit committee and making surveillance between them.Do produce necessary education in order to prevent fraud and describe the duties of official members against fraud.Public awareness of prospective, individual and social rights, processes, standards, ethics frame work of organizations and professional behavior regulation.To support fraud informants and witnesses of company and try to praise.To introduce more efforts in improving official, management, social and cultural elements in order to prevent main causes of fraud.In the case of official and management elements some recommendations are suggested as follow:Reviewing and improvement of vales and regulation and so renewal of organization constructions and designs.To compile the regulation of management promotion and appointment based on their efficiency.Employees performance measurement regulation.The reinforcement of internal control and maximization of control in several organizational units or sections.Employees education in order to maintain dada and electronic information by mentioned items in table (2-2).

XXI. REFERENCES

.

1. Abbott, L., Parker, S., Peters, G., 2004.Audit committee characteristics and restatements. Auditing: A Journal of Practice and Theory 23 (1), 69–87.
2. ACFE and Peltier-Rivest, D. (2007), "Detecting occupational fraud in Canada: a study of its victims and perpetrators", Association of Certified Fraud Examiners, Austin, TX, USA, p. 2.
3. AICPA. SAS No. 82, Consideration of Fraud in a Financial Statement Audit (AICPA 1997).
4. Albrecht W. S., Wernz G. W. and Williams T. L. 1995. Fraud: bringing light to the dark side of business. NY, NY: Richard Irwin.
5. Albrecht, W.S. and Romney, M.B. (1986), "A red-flagging management fraud: a validation", Advances in Accounting, Vol. 3, pp. 323-33.
6. American Institute of Certified Public Accountants (1988), Statement on Auditing Standards No. 53, The Auditor's Responsibility to Detect and Report Errors and Irregularities, AICPA, New York, NY.
7. American Institute of Certified Public Accountants (1997), Statement on Auditing Standards No. 82, Consideration of Fraud in a Financial Statement Audit, AICPA, New York, NY.
8. American Institute of Certified Public Accountants (AICPA). SAS No. 53, The Auditor's Responsibility to Detect and Report Errors and Irregularities (AICPA 1988).
9. American Institute of Certified Public Accountants. 2002. SAS 99: Consideration of Fraud in a Financial Statement Audit. New York, NY: AICPA.
10. Apostolou, B., Hassell, J., Webber, S. and Sumners, G. (2001), "The relative importance of management fraud risk factors", Behavioral Research in Accounting, Vol. 13, pp. 1-24.
11. Arens, A. and Loebbecke, J. (1997), Auditing: An Integrated Approach, Prentice-Hall, Englewood Cliffs, NJ.
12. Association of Certified Fraud Examiners (ACFE) (1996), Report to the Nation on Occupational Fraud and Abuse (The Wells Report), ACFE, Austin, TX
13. Association of Certified Fraud Examiners (ACFE). 2002. 2002 Report to the nation: occupational fraud and abuse.
14. Bayer, J. A. (2002). Fall From Grace: Joe Berardino Presided Over The Biggest Accounting Scandals Ever And The Demise Of a Begendary Firm. Here's What Happened. Business Week 3795(August12), p. 50.
15. Biggs, S., Mock, T., & Watkins, P. (1988). Auditor's use of analytical review in audit program design. The Accounting Review, January, 148±161.
16. Bloomfield, R. J. (1995). Strategic dependence and inherent risk. The Accounting Review (January), 71–90
17. Blue Ribbon Committee (BRC), 1999. Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees. Stamford, CT: BRC.
18. Carcello, J., Neal, T., 2000. Audit committee composition and auditor reporting. The Accounting Review 75 (4), 453–467.
19. Carpenter, B.W. and Mahoney, D.P. (2001), "Analyzing organizational fraud", Internal Auditor, April, pp. 33-38.
20. Ceci S. J., Leichtman M. D. and Putnick M. E. 1992. Cognitive and Social Factors in Early Deception. Hillsdale, NJ: Lawrence Erlbaum Associates.
21. Chen, C. and Sennetti, J. (2005), "Fraudulent financial reporting characteristics of the computer industry under a strategic-systems lens", Journal of Forensic Accounting, Vol. VI No. 1, pp. 23-54.
22. Chi, M., Glaser, R., & Rees, E. (1982). Expertise in problem solving. In R.J. Sternberg, Advances in the psychology of human intelligence. Hillsdale, NJ: Erlbaum.
23. Christ, M. (1993). Evidence on the nature of audit planning problem representations: an examination of auditor free recalls. The Accounting Review, April, 304±322.
24. Cordato, R. E. (1991). Destroying real estate through the tax code (Tax reform act of 1986). The CPA Journal (June), 8.
25. Cosmides L. 1989. The logic of social exchange: Has natural selection shaped how humans reason? Studies with the Wason selection task. Cognition, 31, 187-276.
26. Cosmides L., Tooby J. 1992. Cognitive adaptations for social exchange. In J. Barkow, L. Cosmides, J. Tooby (Eds.) The Adapted Mind, New York, NY: Oxford University Press, 163-228.
27. Costello, J.L. (1991), "The auditor's responsibilities for fraud detection and disclosure: do the auditing standards provide safe harbor? *Maine Law Review*, Vol. 43, pp. 265-305.
28. DeZoort, F., Salterio, S., 2001. The effects of corporate governance experience and financial reporting and audit knowledge on audit committee members' judgments. Auditing: A Journal of Practice and Theory 20 (2), 31–47.
29. Durtschi, C., Hillison, W. and Pacini, C. (2004), "Effective use of Benford's law in detecting fraud in accounting data", Journal of Forensic Accounting, Vol. V No. 1, pp. 17-34.
30. Ekman P. 1992. Telling Lies: Clues to Deceit in the Market Place, Politics, and Marriage. NY, NY: W. W. Norton and Company.

32. Gerard, G., Hillison, W. and Pacini, C. (2004), "Identity theft: the US legal environment and organisations' related responsibilities", Journal of Financial Crime, Vol. 12 No. 1, pp. 33-43.
33. Hillison, W., C. Pacini, D. Sinason. 1999. The internal auditor as fraud-buster. Managerial Auditing Journal. 14 (7): 351-364.
34. Holtfreter, K. (2004), "Fraud in US organisations: an examination of control mechanisms", Journal of Financial Crime, Vol. 12 No. 1, pp. 88-95.
35. Hubert D. Glover and June Y. Aono(1995) Changing the model for prevention and detection of fraud, Managerial Auditing Journal, Vol. 10 No. 5, 1995, pp. 3-9
36. James L. Bierstaker, Richard G. Brody, Carl Pacini, "Accountants' perceptions regarding fraud detection and prevention methods", Managerial Auditing Journal, Vol. 21 No. 5, 2006.
37. Kalbers, L., Fogarty, T., 1993. Audit committee effectiveness: an empirical investigation of the contribution of power. Auditing: A Journal of Practice & Theory 12 (1), 24–49.
38. Kinney, W. R., Jr., Palmrose, Z.-V., & Scholtz, S. (2004). Auditor independence, non-audit services, and restatements: Was the U.S. government right? Journal of Accounting Research, 42(3), 561–588.
39. Knapp, C. (1995). The use of fraud schema during analytical procedures: effects of experience, client explanations and attention cues. Unpublished dissertation, University of Oklahoma.
40. KPMG Peat Marwick (1998), 1998 Fraud Survey, KPMG.
41. Krishnan, J., 2005. Audit committee financial expertise and internal control: an empirical analysis. The Accounting Review 80 (2), 649–675.
42. Kunitake, W. K. (1987). SEC accounting-related enforcement actions 1934–1984: A summary. Research in Accounting Regulation, 79–87.
43. Lanza, R. (2000), "Using digital analysis to detect fraud", Journal of Forensic Accounting, Vol. I No. 2, pp. 291-6.
44. Leibs, S. 2004. New Terrain. CFO Magazine. March.
45. Libby, R., & Frederick, D. (1990). Experience and the ability to explain audit findings. Journal of Accounting Research, Autumn, 348±346
46. Loebbecke, J.K. and Willingham, J.J. Jr (1988), Review of SEC Accounting and Auditing Enforcement Releases, working paper, University of Utah, Utah.
47. Moeckel, C. (1990). The effect of experience on auditors' memory errors. Journal of Accounting Research, autumn, 368±387.
48. Mokhiber, R., Corporate Crime and Violence: BigBusiness Power and the Abuse of the Public Trust, SierraClub Books, San Francisco, CA, 1988.
49. Moyes, G. and Baker, C.R. (2003), "Auditors' beliefs about the fraud detection effectiveness of standard audit procedures", Journal of Forensic Accounting, Vol. IV No. 2, pp. 199-216.
50. Mulligan, T.S. (2002). Accounting Watchdog Reiterates it will Disband. Los Angeles Times, February.C4.
51. National Commission on Fraudulent Financial Reporting (1987). Report of the national commission on fraudulent financial reporting.
52. Palmrose, Z. (1991), "Trial for legal disputes involving independent auditors: some empirical evidence", Journal of Accounting Research, Vol. 29, pp. 149-85.
53. Pergola, C.W. and Sprung, P.C. (2005), "Developing a genuine anti-fraud environment", Risk Management, Vol. 52 No. 3, p. 43.
54. Perry, L. J., and B. J. Bryan. 1997. Heightened responsibilities of the internal auditor in the detection of fraud. Managerial Finance. 23 (12): 38-43.
55. Peterson, B.K. and Buckhoff, T.A. (2004), "Anti-fraud education in academia", Advances in Accounting Education: Teaching and Curriculum Innovations, Vol. 6, pp. 45-67.
56. PriceWaterhouseCoopers (PWC) (2003), Global Economic Crime Survey 2003, available at: www. pwcglobal.com/extweb/ncsurvers.nsf
57. Primoff, W. M. (1992). Year-end accounting and auditing advantage. The CPA Journal Online. January. New York, NY: The New York State Society of CPA.
58. Raghunandan, K., Read, W., Rama, D., 2001. Audit committee composition, „gray directors,'' and interaction with internal auditing. Accounting Horizons 15 (2), 105–118.
59. Ratliff, R., W. Wallace, G. Sumner, W. McFarland, and J. Loebbecke. 1996. Internal Auditing: Principles and Techniques, 2nd ed., The Instititute of Internal Auditors, Altamonte Springs, FL.
60. Restatements: Was the U.S. government right? Journal of Accounting Research, 42(3), 561–588.
61. Rezaee, Z., Crumbley, D.L. and Elmore, R.C. (2004), "Forensic accounting education", Advances in Accounting Education: Teaching and Curriculum Innovations, Vol. 6, pp. 193-231.
62. Scarbrough, D., Rama, D., Raghunandan, K., 1998. Audit committee composition and interaction with internal auditing: Canadian evidence. Accounting Horizons 12 (1), 51–62.
63. Temple, R. M. (1992). Auditors as business advisors: Logical extension of SAS 55. The CPA Journal Online. January. New York, NY: The New York State Society of CPA.
64. Thomas, A.R. and Gibson, K.M. (2003), "Management is responsible, too", Journal of Accountancy, April, pp. 53-55.
65. Tubbs, R. (1992). The effect of experience on the auditor's organization and amount of knowledge. The Accounting Review, October, 783±801.
66. U.S. Chamber of Commerce (2003). Comments on File No. S7-49-02 proposed rule: Strengthening the commission's requirements regarding auditor independence. Washington, D.C.

67. U.S. Securities and Exchange Commission (SEC). (2003). Final Rule: Strengthening the Commission's Requirements Regarding Auditor Independence. 17 CFR PARTS 210, 240, 249 and 274 [Release Nos. 33-8183; 34-47265; 35-27642; IC-25915; IA-2103, FR-68, File No. S7-49-02]. Washington, DC: Securities and Exchange Commission.
68. United States General Accounting Office (GAO) (1989). Bank failures – Independent audits needed to strengthen internal control and bank management (May).
69. Vasek M. E. 1986. Lying as a skill: The development of deception in children. In R. W. Mitchell & N. S. Thompson (Eds.) Deception: Perspectives on Human and Non-Human Deceit. Albany, NY: SUNY Press, 271-292.
70. Wilks T., Zimbelman M. 2004. Using Game Theory and Strategic Reasoning Concepts to Prevent and Detect Fraud, Accounting Horizons, 18(3), 173-184.