Detecting Fraud in the Organization: An Internal Audit Perspective

Priscilla Burnaby
Martha Howe
Brigitte W. Muehlmann*

Fraud is a costly problem for organizations. The Association of Certified Fraud Examiners' (ACFE) 2008 survey results reported that U.S. organizations lost an estimated 7% of their annual revenues to fraud (ACFE 2008). This percentage increased from the estimated 5% for 2006 and 6% for 2004 (ACFE 2006). With layoffs and cuts in travel budgets for internal auditors, there is concern that as economic stresses increase due to the poor economy there will be more instances of fraud and corruption (Sullivan 2009).

As organizations work to reduce the incidence of fraud, their anti-fraud programs continue to rely heavily on the internal audit activity. Over time as internal auditors review systems in the organization, they develop an overall knowledge of the organization's processes, risks, control systems and personnel (IIA 2009c). These factors contribute to their effectiveness at detecting fraud.

The ACFE's 2008 survey provides empirical evidence to this effect as the survey found that over 19% of the respondents' fraud cases were initially detected by internal audits versus about 9% that were discovered by external audits. The survey respondents noted that their organizations' internal audit departments played the most important role in uncovering or limiting asset misappropriations and corruption schemes. The internal auditor's role was greater than management review of internal controls, surprise audits, fraud hotlines, rewards for whistleblowers, mandatory job rotation and vacations, and audits of internal controls for financial reporting. Internal audit department's role in detecting or limiting financial statement

* Priscilla Burnaby and Martha Howe are both at Bentley University. Brigitte W. Muehlmann is at Suffolk University.

fraud schemes was ranked second behind rewards for whistleblowers (ACFE 2008). The survey did not address IT as a separate fraud area.

This study first reviews internal auditors' responsibilities for detecting fraud in their organizations. Then the information gathered about the demographics of the respondents and their organizations is presented. The next section examines how internal auditors ranked the likelihood and impact of fraud in their organizations in four areas: financial statement reporting, asset misappropriation, corruption and information technology (IT) and summarizes the audit procedures that respondents indicated they use to detect fraud in each of these areas. Another section lists the types of software used by internal auditors to search for fraud. Finally, the study presents the key skills that respondents suggested are needed by internal auditors for fraud detection.

BACKGROUND

Internal Auditors' Role in Detecting Fraud

The Institute of Internal Auditors (IIA) provides mandatory guidance for internal auditors in its *International Professional Practices Framework (IPPF)* through the *International Standards for the Practice of Internal Auditing (Standards) (IIA 2009a)*. Several Standards outline the role of the internal auditor in detecting, preventing, and monitoring fraud risks and addressing those risks in audits and investigations (IIA 2009c). IIA Standard 1200, *Proficiency and Due Professional Care*, requires that internal auditors have sufficient knowledge to evaluate the risk of fraud in their organizations, but they are not expected to have expertise in fraud detection. IIA Standard 2060, *Reporting to Senior Management and the Board*, requires that internal auditors report to the Board any fraud risks found during their investigations under IIA Standard 2120, *Risk Management*. Finally, IIA Standard 2210, *Engagement Objectives*, states

that when internal auditors are developing engagement objectives, the probability of fraud must be considered (IIA 2009a). This study explores how internal auditors perform audits to fulfill their responsibilities in order to satisfy these IIA Standards.

Likelihood of Occurrence and Financial Impact

One of the goals of an organization's anti-fraud policy is the prevention of fraud. Although it is not feasible to eliminate every possible occurrence, fraud detection is an interrelated goal of an anti-fraud program. The main focus of this research was to determine what areas in their organizations internal auditors perceive to have more or less risk of fraud. Designing controls and procedures to detect fraud starts with the same type of fraud risk analysis that is integral to establishing preventive internal controls. It is important for internal auditors to be able to identify the organization's fraud risks, in terms of both likelihood of occurrence and financial impact to determine which procedures to audit and examine for fraud. The four major fraud risk areas studied were financial statement reporting, asset misappropriation, corruption and IT.

Effective Audit Procedures

Based on an understanding of the fraud risks that confront organizations, detection rests on the implementation of detection methods that respond to those fraud risks as they evolve over time (IIA 2009c). Once internal auditors are concerned with a possible fraud, they need to decide what audit procedures to use when they attempt to determine if a fraud has occurred. IIA Standard 1220, *Due Professional Care*, states that the internal auditor needs to consider the extent of work needed to achieve the audit objectives and the probability of significant errors and fraud (IIA 2009a). To gain an understanding of the audit procedures used by internal auditors,

respondents were asked to list the most effective audit procedures they use to detect fraud in the areas of financial statement reporting, asset misappropriation, corruption and IT.

Use of Technology to Find Fraud

As many perpetrators use technology to carry out their frauds, internal auditors should use technology to detect those misappropriations (IIA 2009b). IIA Standard 1220A2, *Due Professional Care,* specifically mentions the use of technology-based audit techniques (IIA 2009a, 20). Internal auditors may find that several business intelligence tools can be effective for detecting fraud in the identified fraud risk areas. Several such techniques are addressed in The IIA's December 2009 Global Technology Audit Guide (GTAG), "Fraud Prevention and Detection in an Automated World." Due to the importance of this audit technique, the respondents were asked to indicate whether they used IT tools and if so which ones.

Skills Needed by the Internal Auditor to Detect Fraud

While The IIA *Standards* do not require that internal auditors have the expertise of a person whose job it is to detect and investigate fraud, they are expected to have, as mentioned above, "sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization" (IIA 2009a, 19). To determine the types of skills internal auditors feel are needed to audit for and find fraud, respondents were asked to list the three most important skills an internal auditor needs for fraud examination.

The next section reviews the research methodology used in this study and discusses the research questions.

METHODOLOGY

Questionnaire

The survey document in Exhibit I was used to capture the following information for this study:

- The responders' qualifications
- Types of organizations
- Use of intelligence tools to detect fraud
- Skills needed by internal auditors for fraud examination
- The impact and likelihood of fraud in areas of concern
- The audit steps used to find fraud

While a large number of answers were based on a 7-point Likert scale, several of the questions were open-ended to allow respondents to provide information about their organizations' fraud issues or their opinions about what types of audit steps or skills are best to find fraud.

Population

The subjects were internal auditors with varying experience levels and backgrounds. A survey instrument collected demographic information about the respondents and their organizations. The questionnaire was distributed at two of The IIA's Greater Boston Chapter CPE meetings. It was also sent directly to Massachusetts Bank Internal Auditors. There were 48 usable responses. Although this is a small sample, this paper is designed to provide a view of what types of fraud are currently being encountered by internal auditors in their battle to help management detect and prevent fraud.

Research Questions

RQ1: In terms of impact and likelihood, what are internal auditors' perceived fraud risks for their organizations?

As an important first step in developing an anti-fraud program, a comprehensive fraud risk assessment should be completed. In conjunction with input from different perspectives,

including management, general counsel and the audit committee, internal auditors should work together to develop the anti-fraud program (Baker 2007). Assessing fraud risk is a natural role for internal auditors, and one that is in keeping with The IIA's fraud-related Practice Standards (IIA 2009c). With their understanding of the business and its processes, their knowledge of the organization's performance and related pressures, and their ability to assess internal controls (Zikmund 2008), internal auditors' skills and abilities to determine the top fraud risks in terms of likelihood and impact are vital to the company's anti-fraud program.

This fraud assessment is a first step toward designing procedures to prevent and detect fraud. In this study, internal auditors were asked to complete an assessment of the fraud risks for their organization, in terms of likelihood of occurrence and in severity of impact. When there were enough respondents in an industry, analyses were performed to evaluate the subjects' level of consensus of likelihood and risk of each issue between those industries.

RQ2: What procedures are perceived by internal auditors to be the most effective at detecting their organizations' top fraud risks?

Based on the fraud risk assessment, an anti-fraud program ensures that there are adequate controls in place to prevent and detect fraud. Although the goal of prevention is to stop fraud from occurring, it is not cost-effective to prevent all fraud so it is important to have controls that allow for the prompt and effective detection of any material frauds. In some cases, "an organization may choose to design its controls to detect rather than prevent fraud risks" (IIA 2009c, 18). Compared to preventive controls, controls and procedures to detect fraud tend to be less obvious in the organization (IIA 2009c, 21). Apart from red-flag studies, research in this area tends to be less pervasive. This study focuses on the detection aspect by examining the procedures that internal auditors believe are most effective to detect fraud.

RQ3: Do internal auditors use business intelligence tools to detect fraud?

Research suggests internal auditors believe that business intelligence tools are effective. For example, Bierstaker et al. (2006) found that internal auditors and accountants tended to rate these techniques as effective in combating fraud, but the study's subjects also noted that these techniques were not used very frequently, except in the largest organizations. Cook & Clements (2009) shared their concern about the lack of use of the best tools that are available and their hope that internal auditors would develop the skills necessary to continue the fight against fraud by using the best tools available. In The IIA's Global Technology Audit Guide, *Fraud Prevention and Detection in an Automated World*, the use of technology as an audit tool allows the internal auditor to go from using IT as a detective control to a continuous monitoring technique. Data analysis technology allows auditors to examine data for indications of fraud (IIA 2009b). The subjects in this study were asked specifically about their use of such business intelligence tools. These questions provided data to form a clearer picture of the use of information technology by internal auditors to detect fraud.

RQ4: What skills are perceived by internal auditors to be the most effective at detecting their organizations' top fraud risks?

An open-ended question was asked about what skills respondents consider to be most important for internal auditors in terms of fighting fraud. The respondents' list of skills was mapped to the *Internal Auditor Competency Framework* which was compiled by subject matter experts and volunteers. The IIA's Competency Framework outlines the minimum level of knowledge and skills needed to effectively operate and maintain an internal audit activity (IIA 2010)

RESULTS

Demographic Information about Respondents

To determine the respondents' qualifications, they were asked several questions about their level of experience, and the types of certifications they held. Figure 1 shows over 60% of the respondents were highly experienced internal auditors, with at least 6 years of experience in the field (See Figure 1).

As shown in Figure 2, their experience was reflected in their positions held in the internal audit activity. Over half of the respondents were positioned either as audit managers or in the top audit position (such as Audit AVP, Internal Audit Director, Chief Audit Executive.) Most held a relevant professional designation. The CPA designation was the most common (38%), followed by the CIA (31%), the CISA (17%), the CFE (10%), and the CFSA (8%). Based on the above, it appears that the respondents were well qualified to respond to the questionnaire (See Figure 2).

Demographic Information about Respondents' Organizations

Information about the organizations for which the respondents provide internal audit services, either as service providers or as employees, is detailed in Figures 3 through 5. In general, the organizations are varied in terms of size and type. Figure 3 shows that 23% of the respondents were employed at companies that provide internal audit services to client firms. The others perform internal audit services for their employer companies, most of which were publicly traded companies. Smaller numbers were employed at privately held companies, not-for-profit organizations, and governmental entities (See Figure 3).

As shown in Figure 4, over half of the respondents worked in small internal audit departments with 5 or fewer auditors. Over 20% worked in large departments with at least 21 auditors (See Figure 4).

The respondents also indicated the size of their organization in terms of the geographic reach, as shown in Figure 5. About 21% of the organizations were local, about 19% were either state or regional, and the majority (60%) were national or international (See Figure 5).

As another indication of size, respondents were asked about the annual revenues or funding for their organizations. About 29% indicated that their organizations had revenues (or funding) of less than $1 million. At the other extreme, about 25% reported that their organizations had revenues in excess of $1 billion.

The survey also asked for the broad industry classifications of the employer organizations. These classifications are shown in Table 1. Respondents were asked to indicate all industry classifications that applied so that the percentages do not add to 100 percent. The Banking/Financial Services/Credit Union (Banking) industry was selected by almost half of the respondents. Next, in order of their frequency, were the Financial, Accounting and/or Business Services (Accounting) industry, the Manufacturing industry, and the Technology industry. In a later section of the paper, these top four industry groups are highlighted in the analysis of impact and likelihood of fraud in various areas of concern that the respondents' have for their organizations (See Table 1).

Impact and Likelihood of Fraud Risks and Procedures for Fraud Risk Detection

The respondents were provided with a list of fraud risks faced by many organizations. They were asked to indicate the impact and likelihood on a scale of 1 (low) to 7 (high) of each fraud happening in their organization or, if a service provider, at their major client. The list of fraud risks was broken down into four areas: financial statement reporting, asset misappropriation, corruption and IT issues. The auditors were then asked to list the three most important audit procedures they used to find fraud in each area (RQ2). An overall mean response

for all respondents was determined for each risk. To determine if different industries had significantly different concerns for the types of risks, the four industries that had more than five respondents were compared using the F test. These four industries were Banking, Accounting, Manufacturing and Technology.

Financial Statement Reporting Issues

Table 2 lists the means of the impact and likelihood of fraud risks for financial statement reporting issues. The risk with the highest mean (4.8) for all industries for impact was existence of cash and marketable securities but this was not perceived as having a high likelihood (mean 2.9). For all industries, the risk area "timing of revenue recognition" had the highest likelihood (mean 3.5) for potential fraud, and was also perceived to have a large impact (mean 4.6). Although the existence of revenue (mean 4.6) tied for the second financial statement area of concern for impact, the perceived likelihood mean was lower at 3.0 (See Table 2).

When using the F-test to compare the perceived differences of impact and likelihood for the financial statement risks between the four industries, some significant differences were identified. The Banking respondents had their highest impact mean (5.0) for the risk of existence and marketable securities, which makes perfect sense. Their next highest mean for impact was 4.2 for risks surrounding the proper recording of accrued liabilities. The Accounting respondents were significantly more concerned with impact of the existence of revenue (mean 5.8) and existence of cash and marketable securities (5.7). They felt the greatest likelihood of problems was with accrued liabilities properly recorded (mean 4.6). In general, there was more concern in auditing for understatement of liabilities than overstatement of assets.

The Manufacturing and Technology respondents had a significantly higher concern (mean 4.3 and 4.2) for the impact of the risk for appropriateness of reserves for sales

returns/discounts. This seems reasonable as both industries provide a physical product to customers that can be returned. The Technology respondents had a significantly higher mean (6.2) for timing of revenue recognition than the other industries, which is understandable as that industry has had problems in the past determining when to recognize revenue due to their products having some software and/or service components imbedded in their sales price. The mean response to likelihood of this happening was only 3.2. It could be that these companies were aware of this issue and the internal auditors perceived that the controls are adequate. Some other financial statement risks that respondents listed in the other category were C-level suite fraud, intangible assets, available-for-sale investments, footnote issues and derivatives.

The respondents were then asked to list for their financial statement reporting fraud concerns the three most effective audit procedures to detect fraud in the financial statements area. The majority listed particular audit tests such as inventory observation, cut-off tests, tracing to supporting documents and reconciliations. The next audit process selected most by the respondents was internal control reviews, such as SOX testing, review of separation of duties, control monitoring, and reviews of employees that had access to various accounts. The third internal audit procedure selected most was analytical review for period to period revenues and costs, changes between accounts and reasonableness of estimates. Audits of specific processes and risk analysis were the fourth and fifth most frequently listed procedures by the respondents.

Asset Misappropriation Issues

The respondents were next asked about the impact and likelihood of fraud for their organizations in the area of asset misappropriation. Safeguarding of assets is part of the definition of an adequate internal control system. When controls do not mitigate the potential for theft or misuse of assets, organizations can have material losses. As shown in Table 3, the two

areas that all the respondents considered to have the largest impact if a loss occurred in their organization were skimming of incoming funds and payroll accuracy. Both had a mean of 3.7. They were less concerned that these events would occur as skimming had a mean likelihood of 3.1 and payroll a mean of 3.0. For all industries, the area with the highest mean likelihood was appropriateness of expense reimbursement with a mean of 4.0 (See Table 3).

For the four industries, the Accounting sector had a significantly higher mean impact of 5.0 and likelihood of 4.4 for skimming of incoming funds and an impact of 4.2 and likelihood of 4.0 for appropriateness of cash register disbursements. This makes sense as this industry has large cash inflows and outflows. The respondents listed theft of inventory, diversion of funds and prepaid accounts as other areas for concern over asset misappropriation.

To find asset misappropriation fraud, respondents would perform audit steps such as cutoff testing, reconciliations, scan accounts for unusual items, review of wire transfers, and physical inventories. They would perform audits of employee expense reports, payroll and inventory. They suggest the review of controls such as tip hotlines, segregation of duties, treasury transactions, approvals of accounts payable, and management review of work of lower level people.

Corruption Issues

The respondents also provided insights about potential corruption in their organizations. Corruption may occur whenever an employee is authorized to spend an organization's money (Wells, 2003). Table 4 presents the mean results of the survey participants' assessments of the impact and likelihood of conflict of interest, domestic bribery and/or kickbacks and violation of the *Foreign Corrupt Practices Act* (FCPA). Overall for all industries, it appears that the respondents were not very concerned about these three corruption issues for potential fraud. The

perceived impact of conflicts of interest ranked highest (4.0), domestic bribery and/or kickbacks second (3.7) and violation of the *Foreign Corrupt Practices Act* lowest (3.4). They also were not concerned about the likelihood of the three types of corruption occurring as the highest likelihood mean for all industries did not exceed 3.4 for conflicts of interest. The Banking, Manufacturing and Technology industry representatives ranked the impact of the three risk areas in the same order as the means of all respondents. The respondents in the Accounting industry rated the risk of domestic bribery and/or kickbacks highest (4.4), followed by violations of the *Foreign Corrupt Practices Act* (4.0) (See Table 4).

The reported likelihood of corruption issues for all industries was the highest for conflicts of interest (3.4), second highest for domestic bribery and/or kickbacks (3.0) and the lowest for violation of the *Foreign Corrupt Practices Act* (2.6). The results for likelihood followed the same order in the Banking and Manufacturing industries. The respondents in the Accounting industry perceived the likelihood of domestic bribery and/or kickbacks the highest (3.4). In the Technology industry, the likelihood of conflicts of interest (3.6) was the highest. When asked to list other areas of concerns regarding corruption risk in their organizations, the following areas were listed: customer collusion, loan fraud, internal theft and insider trading.

In the open ended question for the top three audit procedures used to detect corruption frauds, the most frequently reported steps were a review of internal controls around the segregation of duties. The priority audit procedures included auditing employees' expense reports, reviewing company policies and following up filed complaints. Others noted they used analytical procedures and risk assessment techniques, looked for weaknesses in internal controls, performed audit tests and in-depth audits. They also reviewed the whistleblower policy and tips submitted to a hotline as the most important audit steps to identify corruption issues. Some

respondents reported observing employees and interviewing as part of an overall risk assessment. Other audit tests that respondents most frequently mentioned were reviewing receiving reports and credit histories.

IT Issues

One of the challenges for auditors is to look beyond manual internal controls and find loopholes in information systems where fraud could occur (IIA, 2009b). Table 5 summarizes the means of the respondents' assessments of IT risk areas of concern for all industries and the top four industries. For all industries, the impact for security over employees' access to the systems or data (5.2) was the highest, followed by security of systems and data in terms of inappropriate external parties (5.1) and physical security of hardware (4.4). The means of the likelihood of fraud occurring were 3.8 for security over employees' access to the systems or data, 3.3 for security of systems and data in terms of inappropriate external parties and 2.9 for physical security of hardware, indicating a low probability of occurrence (See Table 5).

For the four industries, there was no significant difference in impact for each IT issue. The results for financial impact in the Banking and Manufacturing industries followed the same order as all industries. Both the Accounting (6.1) and Technology (5.6) respondents selected the security of systems and data as the issue that would have the most impact for their organizations and rated security over employees' access to the systems or data second (Accounting 5.4 and Technology 5.0) and physical security of hardware third (Accounting 5.1 and Technology 4.0).

For likelihood of issue occurrence, only security of systems and data in terms of inappropriate external parties had a significant difference between the four industries with the Accounting industry respondents ranking the likelihood of occurrence the highest at 3.9. For the Banking industry, the mean responses for security over employees' access to the systems had the

second highest likelihood with a mean of 2.8. In the Manufacturing industry, the mean likelihood of concerns about the security over employees' access to the systems or data (3.0) was the highest of the three issues. The means of likelihood responses in the Technology industry were the same for security over employees' access to the systems or data and physical security of hardware at 3.0 and lower for security of systems and data in terms of inappropriate external parties at 1.8. Three out of four respondents who indicated other IT risk areas were in the Banking industry. Their additional areas of concern were payment card industry (PCI) compliance, Internet fraud utilizing electronic banking product delivery channels, disaster recovery and identity theft.

When asked about audit procedures used to find potential fraud IT areas, respondents reported internal control reviews as the most effective procedures that the internal audit activity performed to detect fraud, followed by risk assessment and audit steps. Among the procedures related to internal controls, reviews of access controls, separation of duties and physical security were reported most frequently. Penetration and vulnerability testing were the most frequently reported audit tests. The risk assessment audit procedures were dominated by assessments of IT risk areas in general and IT security including firewalls and anti-virus software. Some respondents reported that this area in their organizations was covered by external auditors and not by the internal audit activity.

Use of Business Intelligence Tools to Detect Fraud

To determine the extent to which the respondents' organizations used business intelligence tools to find and address their identified fraud risks, they were asked to select all these types of tools used in their internal audit work to detect fraud. Of the 48 respondents, 17 stated that one or more of these tools are used. Figure 6 shows that all 17 respondents used data

mining. This result is consistent with Wang & Yang (2009) who reported an increase in the use of data mining to detect fraud, but lamented an overall underutilization. Seven respondents also used relational reporting and six used online analytical processing. Several respondents selected the "other" option; one respondent complained that all the tools listed were deficient in that the processes only caught the low hanging fruit, another noted that they used MS Access, and a third stated that they monitored email looking for transmission of credit card numbers (See Figure 6).

Most Effective Skills at Detecting Top Fraud Risks

Internal auditing requires a large range of skills. These skills include inherent personal qualities and acquired knowledge and skills (Reding 2007, 1-14). The IIA has issued an *Internal Auditor Competency Framework* (Framework) (IIA 2008) that outlines the minimum level of knowledge and skills needed to effectively operate and maintain an internal audit function. The Framework is organized into four general skill buckets: interpersonal skills, tools and techniques, internal audit standards, theory, and methodology, and knowledge areas. The participants of this study were asked to list from most important to least important the top three skills for an internal auditor to have for fraud investigation. Table 6 provides a summary of the results. The following discussion is organized by the four skill buckets from The IIA Competency Framework and the relevant skills within each bucket that were selected by the respondents. As much as space would allow, the respondents' actual words or phrases were included in the table (See Table 6).

The skill areas most often selected from the Framework were in the tools and techniques bucket in the risk and control assessment techniques category. Skepticism was the most frequent response for all three levels of the most important to third most important skills followed by risk assessment and recognizing fraud opportunities.

The second highest scoring skills selected by respondents from the Framework were from internal audit standards, theory, and methodology bucket in the categories of proficiency and due care. The participants ranked as most important the ability to adapt, awareness, the CFE designation, curiosity, experience, being perceptive, suspicious and understanding. The second most important skills included awareness and knowledge. The responses in the third-most important category were common sense, intelligence, creative thinking, curiosity, detail orientation, dogged determination, being naturally suspicious and keeping an open mind that fraud may happen and the internal auditor must be willing to look for it.

Another set of skills from the tools and techniques bucket in data collection and analysis tools and techniques were the third most selected type of skills. Respondents listed analytical skills in the category as the top skill to discover fraud at all three levels. Other skills listed included data analysis, fraud investigation skills and observation. Individual respondents reported imaginative testing, documenting evidence and obtaining relevant data as the third most important skill.

Also in the tools and techniques bucket, the fourth area of most effective skills to find fraud was problem solving tools and techniques. Skills listed by respondents were thinking outside the box, digging deeper, understanding and elevating concerns, recognizing an answer that needs further investigations or information proof, understanding patterns, evaluating the results from the gathered data and problem solving skills. Please review Table 6 for other skills listed as important by respondents.

SUMMARY AND CONCLUSIONS

This paper provides insights gained from a survey of internal auditors into how they perform audits to fulfill their professional responsibilities and the skills that are most important

to find fraud. Across all industries, respondents listed fraud in the IT area as having the greatest potential for large losses with a high likelihood of occurrence. The respondents were most concerned with data and systems security due to inappropriate access by employees and by external parties. Media attention to recent large losses at TJX and other companies due to IT issues are a very real concern for loss of reputation for organizations. The IIA has placed great emphasis on IT fraud as reflected in its recent GTAG, "Fraud Prevention and Detection in an Automated World" (IIA, 2009b). Respondents are aware of the potential impact of losses. The relatively high likelihood ratings may also indicate that auditors are not particularly confident that the organization can prevent or detect an IT fraud in time to mitigate any losses.

Respondents indicated the impact of fraud across all industries was highest in cash and marketable securities, timing of revenue recognition and existence of revenue. The fraud issue with the highest impact rating in the entire survey was the timing of revenue recognition in the Technology and Manufacturing industries. This is not unexpected since inappropriate revenue recognition has been a factor in many infamous financial statement frauds over the past decade. It appears that despite years of attention, prevention measures have not been sufficient to reduce the likelihood of fraud in revenue recognition.

Responses in the asset misappropriation and corruption areas showed few notable results except for Accounting organization respondents that were concerned with the skimming of incoming funds. Employee expense reimbursements were rated the fraud risk with the highest likelihood in the entire survey for all the industries with Technology industry respondents indicating the highest likelihood of the four industries. This may be because expense reimbursements to employees is an area where internal auditors have to rely on the honesty of individuals.

None of the corruption issues were perceived to have a great impact or likelihood, and there were no industry differences in this area. Violation of the *Foreign Corrupt Practices Act* was rated with a very low likelihood, a result that is perhaps due to the relatively low (34%) percentage of respondents from organizations of international reach.

The audit procedures listed by respondents as the most effective to find fraud ranged from review of separation of duties and tests of controls to analysis of risks in the area under audit. For financial statement asset reporting and asset misappropriation, audit procedures included reconciliations and cut-off tests. Audit procedures for corruption were centered around whistleblower policies and observing employees. For audit steps to find IT fraud, respondents listed reviewing controls over physical security and penetration and vulnerability testing. When respondents were asked about the business intelligence tools used to detect fraud, a surprisingly few relied on such tools. Only 35% of the respondents used data mining. It would be interesting to pursue this further by trying to determine whether cost, lack of skills or other reasons lie behind the low utilization of IT tools to detect fraud.

Finally, internal auditors were asked to list the top three skills needed to be the most effective at detecting their organizations' top fraud risks. The responses were loosely mapped into the four buckets of The IIA's Framework for internal auditors' skills: knowledge, tools and techniques, internal audit standards, theory, and methodology, and interpersonal skills. The respondents tended to value "soft" skills and behaviors as opposed to factual knowledge. Skills in "tools and techniques" were listed the most often. Although some of the items within this category are related to factual knowledge, many of the items are more closely related to behaviors or generic skills such as skepticism, putting yourself in the fraudster's shoes and ability to look at something logically. Many responses fell into the area of "internal audit

standards, theory, and methodology." These items frequently tend to be aligned with softer skills and behaviors including curiosity, independence, objectivity, and creative thinking. Finally, some of the respondents listed skills that were mapped within the category of interpersonal skills, such as interviewing and listening.

Although this study had a small sample of internal auditors so that generalizations to all internal auditors should be limited, it is a beginning on gaining an understanding of which areas of potential frauds are incorporated into internal audits, internal auditors' perceptions of the impact and likelihood of these frauds and the types of skills needed by internal auditors to find fraud. It appears that the respondents were planning their audits with the risk of many types of fraud in mind. Further research should replicate this study with a larger population using individuals from large and small internal audit activities to determine if those with more resources and larger organizations use different audit techniques to test for fraud.

REFERENCES

Association of Certified Fraud Examiners. 2006. *Report to the Nation: Occupational Fraud and Abuse*. Austin, TX.

Association of Certified Fraud Examiners. 2008. *Report to the Nation: Occupational Fraud and Abuse*. Austin, TX.

Baker, N. 2007. The fraud disconnect. *Internal Auditor*. 64(2): 38-44.

Bierstaker, J., R.G.Brody & C. Pacini. 2006. Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal* 21(5): 520-536.

Cook, G.J. & L.H. Clements. 2009. Computer-based Proactive Fraud Auditing Tools. *Journal of Forensic & Investigative Accounting* 1(2).

Institute of Internal Auditors. (2008) *Internal Auditor Competency Framework*. Available at: http://www.theiia.org/guidance/additional-resources/competency-framework-for-internal-auditors/.

_____. 2009a. *International Professional Practices Framework*. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.

_____. 2009b. *Global Technology Audit Guide: Fraud Prevention and Detection in an Automated World*. Altamonte Springs, FL.

_____. 2009c. *IPPF Practice Guide: Internal Auditing and Fraud*. Altamonte Springs, FL.

Reding, K.F., P.J. Sobel, U.L. Anderson, M.J. Head, S. Ramamoorti & M. Salamasick. 2007. *Internal Auditing: Assurance & Consulting Services*. The Institute of Internal Auditors Research Foundation, Altamonte Springs, FL.

Sullivan, K. 2009. As Internal Audit Staffs Shrink, Will Fraud Rise? *CFO.com*: CFO Publishing Corporpation.www.cfo.com/printable/article.cfm/14461787.

Wang J. and J.G.S. Yang. 2009. Data Mining Techniques for Auditing Attest Function and Fraud Detection. *Journal of Forensic & Investigative Accounting* 1(1).

Wells, J.T. 2003. Corruption: Causes and Cures. *Journal of Accountancy*. 195(3): 49-52.

Zikmund, P. 2008. 4 steps to a successful fraud risk assessment. *Internal Auditor*. 65(1): 60-64.

FIGURE 1
Respondents' Experience Levels

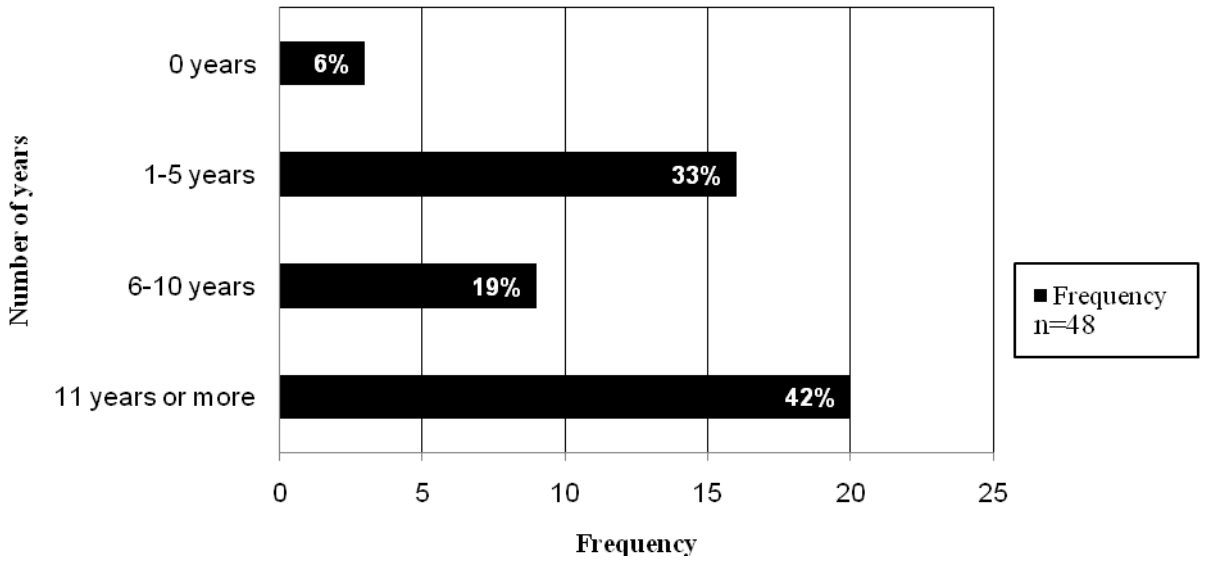

FIGURE 2
Respondents' Positions in Their Organizations

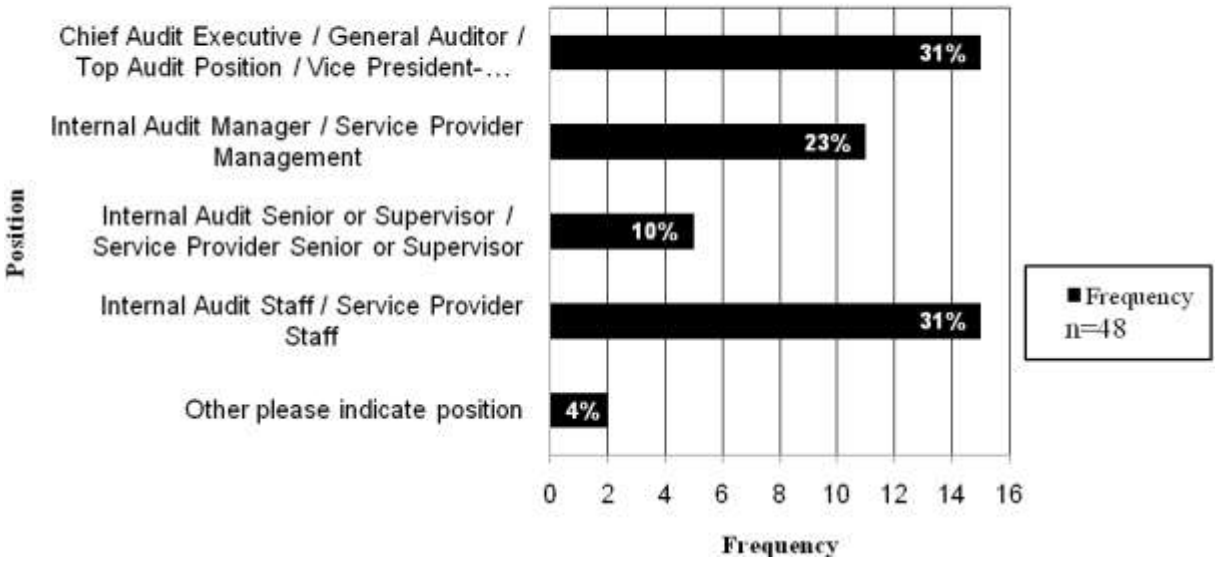

FIGURE 3
Type of Organization in which Respondents Perform Audit Services

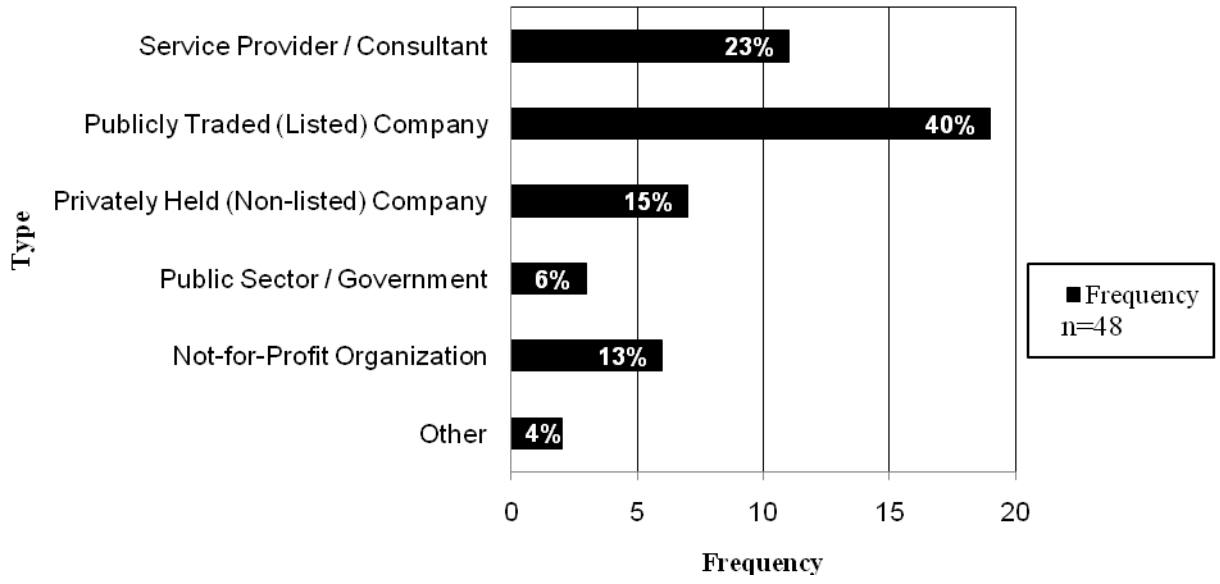

FIGURE 4
Number of Auditors in Internal Audit Department / Professional Services Department

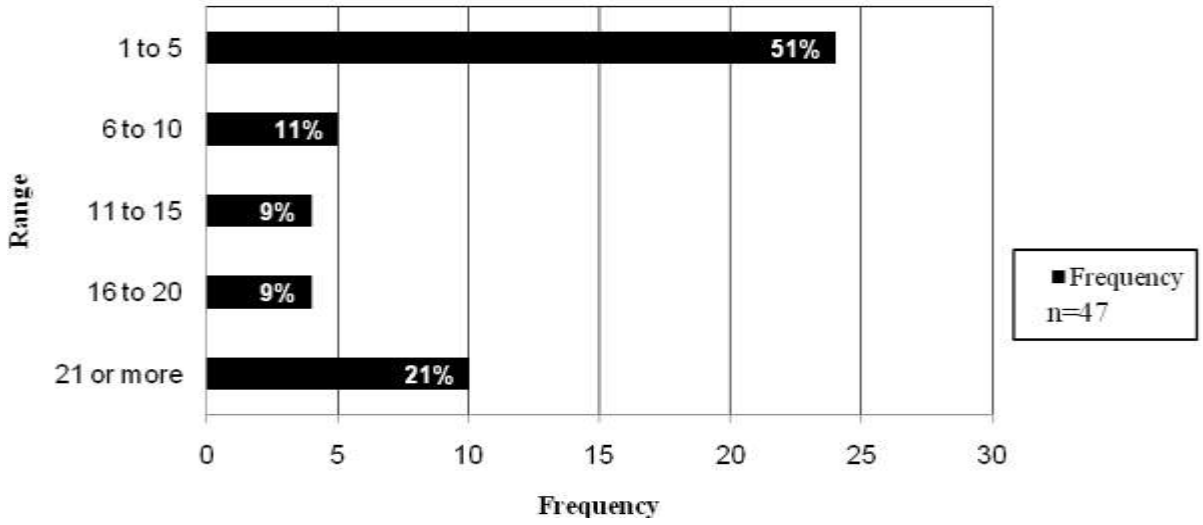

FIGURE 5
Geographic Reach of Respondents' Organizations

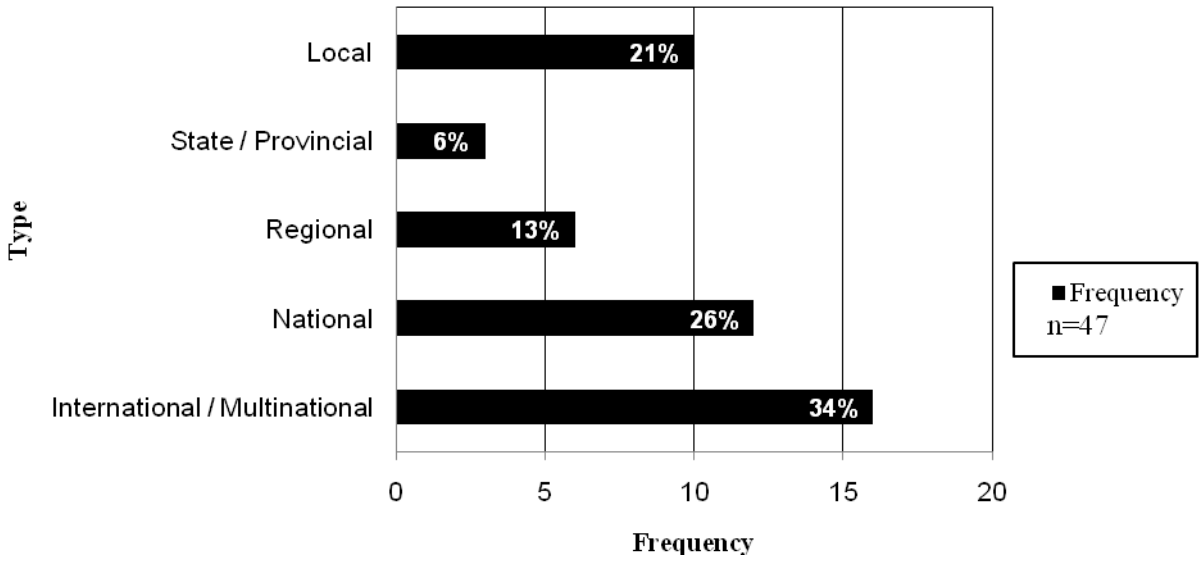

FIGURE 6
Business Intelligence Tools Used to Detect Fraud

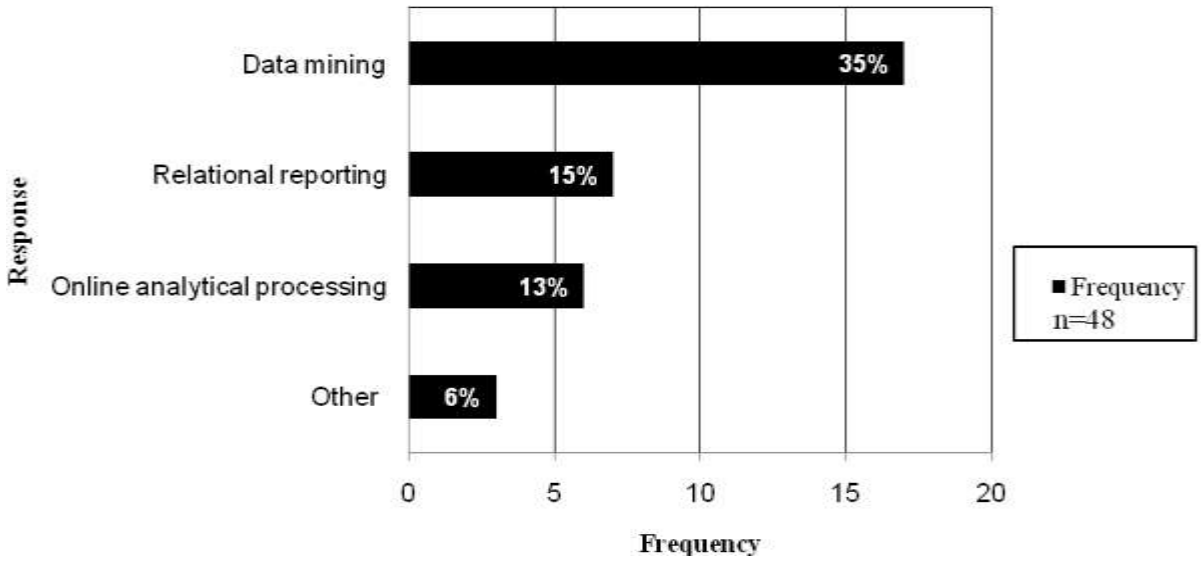

TABLE 1
Industry Classifications of Respondents' Organizations

Industry	Frequency	Percent
Agricultural / Forestry	2	4.2
Banking / Financial Services / Credit Union	22	45.8
Building and Construction	1	2.1
Education	3	6.3
Financial, Accounting, and/or Business Services	9	18.8
Government	4	8.3
Healthcare	5	10.4
Hospitality / Leisure / Tourism	1	2.1
Insurance	3	6.3
Manufacturing	6	12.5
Not-for-Profit	2	4.2
Pharmaceutical / Chemical	1	2.1
Professional Services	1	2.1
Real Estate	1	2.1
Retail / Wholesale	2	4.2
Technology	6	12.5
Trade Services	1	2.1
Transport and Logistics	1	2.1
Utilities	2	4.2

TABLE 2
Risk Areas of Concern: Financial Statement Issues Impact and Likelihood

	All Industries		Banking, Financial Services/ Credit Union		Financial, Accounting, and/or Business Services		Manufacturing		Technology			
Issues	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**F (F)**	**P (P)**
Existence of cash and marketable securities	42	4.8 (2.9)	19	5.0 (3.4)	7	5.7 (2.0)	6	4.3 (2.5)	6	5.7 (2.7)	1.064 (1.833)	0.377 (0.159)
Timing of revenue recognition	44	4.6 (3.5)	19	3.6 (2.9)	8	5.3 (5.6)	6	5.7 (3.3)	6	6.2 (3.2)	4.148 (5.293)	.013** (0.004***)
Existence of revenue	45	4.6 (3.0)	20	3.9 (3.0)	8	5.8 (3.1)	6	5.3 (2.7)	6	5.2 (2.3)	3.257 (0.448)	.032** (0.720)
Accrued liabilities properly recorded	44	4.1 (3.4)	20	4.2 (3.6)	7	5.1 (4.6)	6	3.8 (3.3)	6	3.7 (3.8)	1.111 (0.805)	0.357 (0.499)
Contingent liabilities properly recorded/disclosed	42	4.1 (3.2)	18	3.9 (3.2)	7	5.1 (3.6)	6	4.2 (3.5)	6	3.8 (3.5)	1.080 (0.231)	0.371 (0.874)
Recording of accounts payable	45	3.9 (3.3)	20	3.9 (3.3)	8	4.3 (4.1)	6	4.0 (2.7)	6	3.8 (3.2)	0.091 (1.045)	0.965 (0.384)
Existence of recorded inventory	41	3.8 (2.8)	16	2.9 (2.4)	7	4.9 (3.6)	6	4.2 (2.8)	6	3.7 (2.5)	1.345 (1.031)	0.277 (0.392)

(continued on next page)

TABLE 2 (continued)
Risk Areas of Concern: Financial Statement Issues Impact and Likelihood

	All Industries		Banking, Financial Services/ Credit Union		Financial, Accounting, and/or Business Services		Manufacturing		Technology			
Issues	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**F (F)**	**P (P)**
Appropriateness of accounts receivable allowance for doubtful accounts	44	3.7 (3.2)	20	3.9 (3.2)	8	4.1 (4.1)	6	4.0 (3.2)	6	3.2 (3.2)	0.643 (1.058)	0.592 (0.379)
Capitalization versus expensing of costs	44	3.5 (3.2)	20	3.8 (3.4)	7	4.3 (4.3)	6	3.7 (3.5)	6	3.0 (3.5)	0.717 (0.359)	0.548 (0.783)
Appropriateness of reserve for sales returns/discounts	39	3.1 (2.7)	16	2.4 (2.3)	8	3.8 (3.5)	6	4.3 (3.2)	6	4.2 (3.0)	2.434 (0.769)	.082* (0.519)
Existence of fixed assets	43	3.0 (2.4)	19	2.8 (2.2)	7	4.0 (2.3)	6	2.3 (2.2)	6	2.3 (2.7)	1.486 (0.186)	0.235 (0.905)
Obsolete inventory not properly recorded	42	2.9 (3.0)	17	2.0 (2.2)	8	3.5 (4.6)	6	4.0 (3.2)	6	3.0 (2.5)	2.342 (3.928)	0.091* (0.016**)

Differences in means are tested by one-way ANOVA. *, **, and *** denote the statistical significance of F statistics at 0.1, 0.05, and 0.001 levels respectively.
The tests were performed for the four industries excluding the results for all industries.

TABLE 3
Risk Areas of Concern: Asset Misappropriation Issues Impact and Likelihood

	All Industries		Banking, Financial Services/ Credit Union		Financial, Accounting, and/or Business Services		Manufacturing		Technology			
Issues	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**F (F)**	**P (P)**
Skimming of incoming funds	41	3.7 (3.1)	20	3.0 (2.4)	7	5.0 (4.4)	5	4.2 (1.8)	5	4.2 (1.8)	1.478 (5.312)	0.238 (0.004***)
Payroll accuracy	43	3.7 (3.0)	20	3.6 (3.3)	7	3.7 (2.9)	5	3.8 (2.2)	5	4.0 (3.2)	0.221 (0.467)	0.881 (0.707)
Appropriateness of payments to vendors	44	3.6 (3.6)	20	3.6 (3.6)	8	3.8 (4.3)	5	4.0 (3.2)	5	4.0 (3.0)	0.290 (0.528)	0.832 (0.666)
Appropriateness of expense reimbursements to employees	42	3.0 (4.0)	21	3.2 (4.1)	8	3.0 (4.1)	5	3.2 (3.6)	5	3.2 (5.2)	0.176 (0.920)	0.912 (0.441)
Appropriateness of cash register disbursements (voids, returns, etc.)	35	2.5 (2.9)	15	1.7 (1.8)	6	4.2 (4.0)	6	2.0 (2.2)	5	1.8 (2.4)	3.765 (2.247)	0.021** (0.105)

Differences in means are tested by one-way ANOVA. **, and *** denote the statistical significance of F statistics at 0.05, and 0.01 levels respectively.
The tests were performed for the four industries excluding the results for all industries.

TABLE 4
Risk Areas of Concern: Corruption Issues Impact and Likelihood

	All Industries		Banking, Financial Services/ Credit Union		Financial, Accounting, and/or Business Services		Manufacturing		Technology			
Issues	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**F (F)**	**P (P)**
Conflicts of interest	45	4.0 (3.4)	21	4.3 (3.1)	8	3.6 (2.5)	5	4.0 (2.6)	5	4.2 (3.6)	0.461 (0.873)	0.711 (0.464)
Domestic bribery and/or kickbacks	44	3.7 (3.0)	21	3.4 (2.9)	8	4.4 (3.4)	5	3.8 (2.2)	5	4.0 (2.4)	0.674 (0.596)	0.574 (0.622)
Violation of *Foreign Corrupt Practices Act*	39	3.4 (2.6)	20	3.1 (2.5)	7	4.0 (2.4)	5	3.0 (1.8)	5	3.8 (3.0)	0.325 (0.261)	0.807 (0.853)

Differences in means are tested by one-way ANOVA. The F statistics are not significant at 0.1, 0.05 or 0.01 levels.
The tests were performed for the four industries excluding the results for all industries.

TABLE 5
Risk Areas of Concern: Information Technology Issues Impact and Likelihood

	All Industries		Banking, Financial Services/ Credit Union		Financial, Accounting, and/or Business Services		Manufacturing		Technology			
Issues	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**n**	**Impact (Likelihood)**	**F (F)**	**P (P)**
Security over employees' access to the systems or data	44	5.2 (3.8)	20	5.5 (3.5)	7	5.4 (4.3)	5	5.2 (3.0)	5	5.0 (3.0)	0.079 (1.000)	0.971 (0.405)
Security of systems and data in terms of inappropriate external parties	44	5.1 (3.3)	20	4.9 (2.8)	7	6.1 (3.9)	5	4.2 (1.8)	5	5.6 (2.4)	1.438 (2.619)	0.249 (0.067*)
Physical security of hardware	44	4.4 (2.9)	20	4.7 (2.5)	7	5.1 (3.0)	5	3.4 (2.0)	5	4.0 (3.0)	1.178 (0.384)	0.332 (0.765)

Differences in means are tested by one-way ANOVA. * denotes the statistical significance of F statistics at the 0.1 level. The tests were performed for the four industries excluding the results for all industries.

TABLE 6
Internal Auditors' Perceptions of Most Effective Skills for the Detection of Top Fraud Risks at Their Organizations

Skill	Most Important (number of responses)	Second most Important (number of responses)	Third most Important (number of responses)
Interpersonal skills			
Influence			Ability to educate management regarding risks of fraud (1)
Communication	Interviewing (3) Listening (1)	Interviewing (6) Listening (1)	Interviewing (1) Communication in general (1)
Management			Interpersonal skills in general (1)
Collaboration and cooperation	Communicating with & understanding company employees (1)		Structural approach (1) Tact (1)
Tools and techniques			
Operational and management research tools		Research (1)	
Business process analysis		Analyzing business processes (1) Visualizing a process (1)	
Risk and control assessment techniques	Skepticism (6) Recognizing potential fraud opportunities (2) Risk assessment (2) Recognizing fraud (1) Risk identification (1)	Skepticism (5) Perceiving behaviors (2) Ability to look at something logically (1) Creating scenarios (1) Identifying risk (1) Judging (1) Materiality (1)	Skepticism (3) Putting yourself in the fraudsters shoes (1)
Data collection and analysis tools and techniques	Analytical skills (4) Data analysis (1)	Analytical skills (4) Data analysis (1) Fraud investigation skills (1) Observation (1)	Analytical skills (4) Documenting evidence (1) Imaginative testing (1) Obtaining relevant data (1)
Problem solving tools and techniques	Thinking outside the box (1)	Digging deeper (1) Escalation (1)	Evaluating the results from the gathered data (1) Problem solving skills in general (1) Recognizing an answer that needs further investigations or information proof (1) Thinking outside the box (1) Understanding and elevating concerns (1)\ Understanding patterns (1)

(continued on next page)

TABLE 6 (continued)
Internal Auditors' Perceptions of Most Effective Skills for the Detection of Top Fraud Risks at Their Organizations

Skill	Most Important (number of responses)	Second most Important (number of responses)	Third most Important (number of responses)
Internal audit standards, theory, and methodology			
Purpose, authority, and responsibility	Independence (1) Objectivity (1)	Independence (1) Objectivity (1) Thoroughness (1)	
Proficiency and due professional care	Ability to adapt (1) Awareness (1) CFE designation (1) Curiosity (1) Experience (1) Perceptive (1) Suspicion (1) Understanding (1)	Awareness (2) Knowledge (1)	Common sense (1) Intelligence (1) Creative thinking (1) Critical thinking (1) Curiosity (1) Detail orientation (1) Dogged determination (1) Naturally suspicious (1) Open mind that fraud may happen and willingness to look for it (1)
Nature of work	Following up on red flags (1)	Attention to details (2) Courage to investigate (1) Inquisitive (1)	Attention to details (1) Courage to pursue questionable transactions and red flags (1) Experience with fraud in the industry (1)
Engagement planning	Knowledge of process (1)		
Performing the engagement	Follow up on red flags (1)	Investigating (1)	Investigating (1)
Communicating results			Reporting findings (1)
Monitoring progress			Monitoring (1)
Knowledge areas			
Financial accounting and finance		Financial reporting (1) Understanding of fundamental accounting (1) Understanding which accounts could be affected (1)	Accounting knowledge (1)
Regulatory, legal, and economics	Understanding of the business (1)	Legal concerns (1) Solid industry knowledge (1)	Legal requirements (1)
Ethics and fraud	Awareness of fraud indicators (1)	Comprehension of fraud concepts and fraud schemes (1)	Knowledge why, where fraud occurs (1)
Information technology	Information technology (1)		

EXHIBIT I
Survey Instrument

Part I Background Information: Background information will be used anonymously for aggregate data analysis. No individual information will be revealed in research reports.

1. The type of organization for which you currently work:
   - Service Provider / Consultant
   - Publicly Traded (Listed) Company
   - Privately Held (Non-listed) Company
   - Public Sector / Government
   - Not-for-Profit Organization
   - Other

2. How long have you been an internal auditor?
   - 1-5 years
   - 6-10 years
   - 11 years or more
   - I am not a an internal auditor

3. Please indicate certifications you hold such as
   - CIA
   - CFE
   - CPA

   Other please list: _____

4. Your position in the organization:
   - Chief Audit Executive / General Auditor / Top Audit Position / Vice President - Audit / Service Provider equivalent
   - Internal Audit Manager / Service Provider Management
   - Internal Audit Senior or Supervisor / Service Provider Senior or Supervisor
   - Internal Audit Staff / Service Provider Staff
   - Support Staff (administration, secretarial, and clerical)
   - Other please indicate position_____

5. Number of Auditors in Internal Audit Department/Professional Services Department:
   - 1 to 5
   - 6 to 10
   - 11 to 15
   - 16 to 20
   - 21 or more

6..Revenue for 2008:
   - < 250 million
   - > 250 Million - 1 Billion
   - > Billion

7. Is your organization:
   - Local
   - State / Provincial
   - Regional

- National
- International / Multinational

8. The broad industry classification(s) of the organization for which you work or provide internal audit services: (Please mark all that apply.)

- Agricultural / Forestry
- Banking / Financial Services / Credit Union
- Building and Construction
- Communication / Telecommunication
- Consumer Goods
- Education
- Financial, Accounting, and/or Business Services
- Healthcare
- Hospitality / Leisure / Tourism
- Insurance
- Manufacturing
- Mining and Oil
- Non-Professional Services
- Pharmaceutical / Chemical
- Professional Services
- Real Estate
- Retail / Wholesale
- Technology
- Trade Services
- Transport and Logistics
- Utilities
- Other

Part II – Fraud Areas of Concern for Your Organization or Clients:

9. Does your organization use business intelligence tools to detect fraud? Yes ___ No ___

If yes, please specify all that apply:

- Data mining
- Relational reporting
- Online analytical processing (OLAP)
- Other please list: _____

10. In terms of fraud examination, what are the three most important skills an internal auditor should have? Please prioritize by listing them in order, with your most important skill first.

1. _____

2. _____

3. _____

11. Listed below are several fraud risks faced by many organizations. Based on the likelihood and impact of a potential fraud please rank from 1 low impact/likelihood to7 high impact/likelihood for your organization or your major client.

Areas of Concern	**Impact (Amount of potential loss) Low 1 to High 7**	**Likelihood (Probability of occurrence) Low 1 to High 7**
Financial Statement Issues :		
Timing of revenue recognition		
Existence of revenue		
Appropriateness of reserve for sales returns/discounts		
Existence of recorded inventory		
Obsolete inventory not properly recorded		
Appropriateness of accounts receivable allowance for doubtful accounts		
Recording of accounts payable		
Accrued liabilities properly recorded		
Contingent liabilities properly recorded/disclosed		
Capitalization versus expensing of costs		
Existence of fixed assets		
Existence of cash and marketable securities		
Other financial statement risk areas please list:		
Asset Misappropriation Issues:		
Skimming of incoming funds		
Appropriateness of cash register disbursements (voids, returns, etc.)		
Appropriateness of payments to vendors		
Payroll accuracy		
Appropriateness of expense reimbursements to employees		
Other asset misappropriation risk areas please list:		
Corruption Issues:		
Violations of *Foreign Corrupt Practices Act*		
Domestic bribery and/or kickbacks		
Conflicts of interest		
Others corruption risk areas please list:		
IT Issues:		
Security over employees' access to the systems or data		
Security of systems and data in terms of inappropriate external parties		
Physical security of hardware		
Others ITT risk areas please list:		

12. For your **Financial Statement Issues** fraud risk areas, what are the three most effective audit procedures used to detect fraud? Please prioritize by listing them in order, with your most effective procedure first.

1. _____

2. _____

3. _____

13. For **Asset Misappropriation Issues** fraud risk area, what are the three most effective audit procedures used to detect fraud? Please prioritize by listing them in order, with your most effective procedure first:

1. _____

2. _____

3. _____

14. For **Corruption Issue** fraud risk area, what are the three most effective audit procedures used to detect fraud? Please prioritize by listing them in order, with your most effective procedure first.

1. _____

2. _____

3. _____

15. For **IT Issues** fraud risk area ,what are the three most effective procedures that your internal audit activity performs to detect fraud? Please prioritize by listing them in order, with your most effective procedure first.

1. _____

2. _____

3. _____