

Impact of IT Auditors' Involvement in Financial Audits

Angel R. Otero

Nathan M. Bisk College of Business

Florida Institute of Technology

150 West University Blvd. Melbourne, FL 32901

aotero@fit.edu

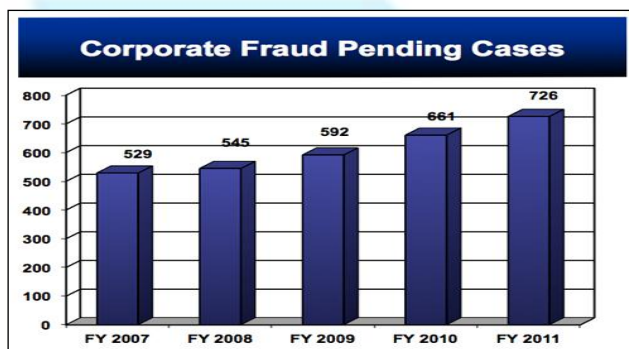
Abstract- Based on the FBI, the majority of corporate fraud cases involve accounting schemes designed to deceive investors, auditors, and analysts about the true financial condition of a corporation. Investigations have determined that companies manipulated their financial systems to fraudulently inflate financial information. Surprisingly, there is limited relevant research requiring the involvement of information technology auditors in financial audits. According to literature, information technology auditors are underused (or not used at all) in financial audits, allowing for opportunities of manipulation, abuse, and/or misreport of financial data. It has been argued that information technology auditors are more likely to effectively understand and test organizations' technology environments than financial auditors. This research investigates whether a relationship exists between inclusion of information technology auditors in financial audits and detecting manipulated financial information in organizations. Results suggest a positive correlation between the above variables, and prompt for additional work to extend the results identified herein.

General Terms- Information Technology, Financial Audits, Information Security

Keywords- Information systems, information technology auditors, internal controls, audits, fraud, manipulation, financial information

1. INTRODUCTION

Nowadays organizations are investing more in information technology (IT) because of the benefits and competitive advantages they provide [46][40]. Studies show that organizations realize positive economic and financial returns as a result of IT investments [35][3]. Nonetheless, studies have also confirmed the harmful effects of unsuccessful IT initiatives and implementations, resulting in increased opportunities for fraud and information security breaches, among others [12][30].



Source: Federal Bureau of Investigation, Financial Crimes Report to the Public Fiscal Year, Department of Justice, US, 2011

Figure 1: US corporate fraud pending cases investigated by the FBI since 2007

The Federal Bureau of Investigation (FBI) reported that in 2011 alone, there were 726 pending corporate fraud cases

in the United States (U.S.) involving accounting schemes designed to deceive investors, auditors, and analysts regarding the true financial condition of a corporation. Figure 1 shows the number of corporate fraud pending cases investigated by the FBI in the U.S. from 2007 through 2011. The U.S. Supplement to the 2014 Global Economic Crime Survey, performed by PricewaterhouseCoopers LLP, featured the views of more than 5,000 participants from over 100 countries on the prevalence and direction of economic crime since 2011. The survey revealed that 54% of U.S. participants reported their companies experienced fraud in excess of \$100,000 with 8% reporting fraud in excess of \$5 million. Similarly, in a study performed by [7], about 21 percent of all deficiencies detected in selected audited organizations were related to IT implementations. Specifically, [7] noted that when implementing IT environments, there were no adequate IT-related controls in place, or the ones in place were not operating effectively.

Adequate selection and implementation of computer controls (general controls and application controls) around IT environments reduce opportunities for failures. Simultaneously, the effective operation of computer controls assists organizations in maintaining a well-designed, controlled, and implemented IT environment. The alarming figures presented above serve as motivation for financial audit teams to assist organizations in ensuring that computer controls exist surrounding these IT and that these controls operate effectively.

According to [1], the following should trigger the inclusion of IT auditors in financial audits:

1. implementation of complex and/or major system changes;
2. significant data sharing;
3. high involvement in e-commerce;
4. employment of emerging technologies; and
5. electronic audit evidence.

[4] also encourage participation of IT auditors to identify whether financial information has been manipulated or abused. Surprisingly, IT auditors are not necessarily involved in financial audits due to restrictions involving costs, resources availability, lack of required IT skills and experience, or simply because financial auditors do not perceive such involvement as necessary. In these cases, financial auditors opt to perform the work themselves which may involve documenting a limited understanding of the IT environment, with some minor level testing of computer controls.

Per[11], the above creates a problem since financial auditors do not have enough knowledge to perform these specialized procedures. [24] state that financial auditors are less likely to understand the control risks resulting from implementation of IT, including enterprise resource planning (ERP) systems. Additionally, [14] indicate that as the complexity of IT increase, there is also "an increased need for auditors to be knowledgeable in more complex IT and controls and, perhaps, an increased need for the involvement of IT specialists in the audit..." (p. 87). [25] also state that inexperienced auditors may fail to measure the degree of risk precisely, resulting in opportunities for organizations' management to easily override controls, manipulate financial information, and/or fraudulently abuse accounting records.

Despite the information presented above, [14] state that there is limited relevant academic research requiring the involvement of IT auditors in financial audits. Furthermore,[27] and [11] state that IT auditors may be underused in financial audits and that such limited involvement allows potential opportunities for manipulation, abuse, and/or misreport of financial data. This research will attempt to determine whether a correlation exists between inclusion of IT auditors in financial audits, and detection of manipulated financial information within organizations' IT environments.

Traditionally, financial audit teams focus on obtaining evidence supporting the preparation of organizations' financial statements, and understanding their financial and IT-related internal control environment. For the latter, financial audit teams have frequently opted not to involve IT auditors due to the additional audit costs, or because they felt confident in performing similar audit procedures surrounding financial systems [24]. Therefore, involvement of IT auditors in financial audits has been relatively low [27][14][11].

[48] and [22] argue that auditors with specialized IT skills and experience are more likely to understand the organization's IT environment than financial auditors and,

most importantly, identify the best computer controls to test IT processes over financial information. The [2] also stated that financial auditors must seek the advice of IT auditors as they lack the necessary skills to properly evaluate computer controls to provide assurance that financial information is represented correctly.

[24] further argue that the financial auditors' lack of adequate understanding of complex IT environments (e.g., ERP systems) increases risks in financial audits. A solid understanding of ERP systems is crucial to support that the financial information generated from these systems is free of errors or misstatements. Based on [24], IT auditors are more capable of identifying risks related to ERP systems and, therefore, draw effective solutions to mitigate those risks. [11] expressed his concern regarding financial auditors lacking adequate IT knowledge/experience, and stressed the significance of IT auditors becoming part of financial audits. Moreover, [22] claim that there is a positive relationship between a well-controlled and managed IT environment and audit costs.

As evidenced above, participation of IT auditors in financial audits is a crucial and necessary audit strategy. Audit teams must comprise professionals with a balanced financial and IT-related understanding. Adequate understanding of IT allows auditors to make an effective selection and testing of computer controls, which may ultimately lead to the detection of manipulated and/or abused financial information.

The remainder of this research is organized as follows: Section two reviews relevant literature regarding IT auditors and manipulation of financial information, as well as develops the hypotheses to be evaluated. Section three describes the research methodology. In section four, finding results are presented and statistically analyzed. Section five discusses the findings, as well as contributions, limitations, and opportunities for future research. Lastly, section six provides the conclusion.

2. LITERATURE REVIEW

The purpose of this section is to review the literature regarding IT auditors role and manipulation of financial information.

2.1 Role of IT Auditors

According to SAS No. 94, audit teams must evaluate organizations' relevant computerized procedures when performing audits [2]. Specifically, SAS No. 94 requires audit teams to:

1. evaluate the impact of the organization's IT infrastructure within the overall audit strategy and
2. design audit tests to determine whether computer controls are implemented adequately and operate effectively.

Furthermore, SAS No. 94 requires auditors to either possess the necessary technical knowledge/ skills to understand, evaluate, and test IT systems, or seek the assistance from specialists.

Financial auditors do not have the technical knowledge necessary to perform IT-related procedures around financial systems [14][27][11]. Due to their lack of expertise in the IT field, financial auditors may feel uncomfortable with understanding and performing computer-related audit procedures [27]. [24] also state that financial auditors are less likely to understand the control risks from IT environments. Moreover, [10] found that auditors with adequate technical knowledge are better at identifying IT-related risks on financial systems, including areas sensitive to fraud or misbehavior by employees.

Based on SAS No. 94, financial auditors must seek the advice of IT specialists when lacking the necessary skills and knowledge to properly evaluate and test IT controls [2]. For instance, given the complexities of an ERP system, inclusion of IT auditors would assist in understanding the IT environment where the ERP is hosted. Most importantly, IT auditors would test computer controls around the ERP system to identify if errors and inconsistencies have resulted from system abuse, manipulation, and/or misreport of financial information [24]. [48] further supports that auditors with specialized IT skills are more likely to understand the organization's IT environment and capable of performing the necessary tests of IT processes.

Experience also plays an important role as organizations feel confident when experienced IT auditors perform audit procedures on their financial systems [27]. Adequate experience is attained when IT auditors perform, as required by the [1], procedures to understand the flow of transactions. IT auditors with relevant experience provide greater assistance to financial audit teams when, for instance, the organization IT controls around financial systems are outsourced [20].

Prior knowledge in auditing IT controls at third parties is a major factor considered by financial audit teams when determining whether to involve IT auditors in financial audits [14] [48]. Experience on how to evaluate the design and operating effectiveness of IT controls at third parties provide financial auditors valuable feedback [20]. For instance, experienced IT auditors can identify concerns related to the appropriateness of the third party; determine whether the organization's financial data is adequately protected; assess whether the organization's financial data has been manipulated or abused; and evaluate the effectiveness of the third party's disaster recovery/business continuity plans [36] [47].

Equally important, reliance can be placed by financial audit teams on the financial systems evaluated and subject to testing by IT auditors [14]. In other words, test procedures performed by experienced IT auditors on controls around organizations' financial information not only mitigate risks, but also provide assurance that procedures have been implemented effectively to protect financial data [45]. With these results, financial auditors can place reliance upon the financial information generated by the organizations' systems, and can perform less

independent test procedures, thus, reducing the amount of hours required for the overall audit work [23] [24].

[45] suggest that IT auditors possess the required knowledge to understand the organizations' financial systems based on their experience performing audits and consultations with clients in specific industries. This provides significant efficiencies to financial audits which may translate into a more relevant and timely work performed [45]. Other researchers like [29] suggest similar conclusions regarding accuracy and efficiencies obtained from experienced IT auditors.

[6] state that efficiencies are realized when auditors with adequate IT experience assist financial audit teams in identifying IT-related audit risks, as well as opportunities for fraud, manipulation of financial information, abuse of systems, etc. than less experienced auditors (financial auditors). [28] reported a positive relationship between utilization of personnel with IT experience and fraud detection. [49] further indicated that IT experience leads to better judgments and greater accuracy when assessing risks and identifying error and irregularities in regards to financial information. Moreover, as there is no single IT solution that can fit all organizations, IT auditors can select appropriate computer controls to fit the specific needs of organizations. Effective selection and testing of the most appropriate computer controls is a major step towards providing an adequate level of assurance that organizations' financial systems are adequately controlled and not subject to manipulation or abuse. The literature just described gives raise to our first variable to be tested: Involvement of IT Auditors.

2.2 Manipulation of Financial Information

Based on the [16], the majority of corporate fraud cases involve accounting schemes designed to deceive investors, auditors, and analysts about the true financial condition of a organization. Recent FBI studies have identified instances of false accounting entries and fraudulently inflated assets and revenues. Investigations have further determined that organizations manipulated their financial systems and used various accounting schemes to inflate their financial reports [16].

By the end of 2011, there were 726 corporate fraud cases involving manipulation and abuse of financial systems throughout the U.S. Several causes of these fraudulent activities include:

1. false accounting entries;
2. bogus trades designed to inflate profit or hide losses; and
3. false transactions designed to evade regulatory oversight. Refer to Figure 1.

Financial statement fraud in particular has experienced a rapid increase by adversely impacting not only on individual investors, but the overall stability of global economies. Financial statement fraud is defined by the Association of Certified Fraud Examiners as "[t]he intentional, deliberate, misstatement or omission of material facts, or accounting data which is misleading and,

when considered with all the information made available, would cause the reader to change or alter his or her judgment or decision.” According to [42], financial statement fraud involves:

1. manipulation of financial systems;
2. intentional omission of events, transactions, accounts, or other significant information from which financial statements are prepared; and
3. abuse or misreporting of financial information.

[14] state that IT auditors have the necessary training and technical skills to assist financial audit teams in determining whether financial systems have been abused or data has been manipulated. In a study performed by [8], professionals from the four large audit firms agreed that IT auditors must keep up with new technologies [14] in order to be able to understand and better assess organizations’ financial systems [8]. The Public Company Accounting Oversight Board (PCAOB) has also noted that audit teams must maintain higher levels of competence with respect to understanding and evaluating financial systems, as well as preventing and detecting fraud [14]. This section of the literature raises to our second variable for testing: Manipulation of Financial Information.

Based on the information, arguments, and claims presented in sections 2.1 and 2.2, the following null (H0) and research (H1) hypotheses are proposed:

- H0: Inclusion of IT auditors in financial audits will not promote effective detection of manipulated financial information within organizations’ IT environments.
- H1: Inclusion of IT auditors in financial audits will promote effective detection of manipulated financial information within organizations’ IT environments.

Figure 2 illustrates the proposed research model. The model depicts a potential relationship between “Inclusion of IT Auditors in Financial Audits” and “Identification of Manipulated Financial Information within IT Environments”.

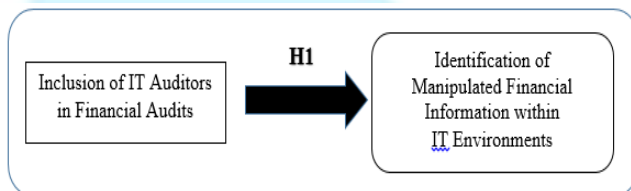


Figure 2: Relationship between participation of IT Auditors and the identification of manipulated financial information in organizations’ IT environments

Section three describes the overall research methodology and rationale for its adoption.

3. RESEARCH METHODOLOGY

This research follows a correlational type of investigation in which one examines the extent to which differences in one variable are related to differences in one or more other

variables [44]. Correlation investigation will help determine whether inclusion of IT auditors in financial audits leads to effective detection of manipulated financial data in organizations’ IT environments. The higher the correlation, the higher will the degree of relatedness be [41].

The research methodology adopted for this study is a 5-point Likert scale survey. Survey approach is used when a series of questions are posed to participants and their responses are summarized with percentages, frequency counts, and/or more sophisticated statistical indexes [32]. Survey approach looks more closely at phenomena of the moment and, therefore, captures responses/feedback from a specific moment in time. Survey research typically employs online assessments, written questionnaires, face-to-face interviews, or telephone interviews [32].

Questionnaires were based on a scale survey which indicated the participant’s level of agreement in regards to the involvement of IT auditors in financial audits and manipulation of financial information. The Likert scale survey examined the level of agreement or disagreement of each participant with statements on a 5-point scale and anchors such as: “Strongly Agree”, “Agree”, “Neutral”, “Disagree”, and “Strongly Disagree” [44]. According to [15], a 5-point scale produces slightly higher mean scores relative to the highest possible attainable score when compared to those produced from a 7-point or 10-point scale.

3.1 Data Collection and Analysis Procedures

In terms of data collection, individuals with financial audit experience were recruited. Requests for participation were made from audit firms located in southeast U.S. The target audience was financial auditors from Staff and Senior level positions through Managers, Directors, Principals, and Partners. Due to their financial audit knowledge and experience, the target audience reflected an accurate representation of the population, allowing for results to be generalizable and consistently applied to other populations with the same characteristics in different settings [41]. Participants were directed to a survey website hosted on a secure server. The data collected was maintained and available only for investigation and analysis purposes. Moreover, to increase confidence, the survey participants were assured that no personal information was attached nor disclosed to their responses and that the data collected was strictly for research purposes. Code numbers were used to ensure that each participant completed only one survey.

The survey questions were developed strictly from the literature review presented in section two. This, in turn, maximized the reliability of the variables under study as well as the results from this research. Additional validation for the questions used in this research included interviews with five subject matter experts with the purpose of reducing ambiguity and increasing the reliability of the questions [44] [39]. Subject matter experts assisted in clarifying and/or explaining the wording for each question.

Questions were added, reworded, or deleted as a result of the experts' reviews.

To test the hypotheses within this study, correlation research was employed. [41] states that to assess the degree of relatedness between two variables, the correlation coefficient is the most frequent measure used. The correlation between the independent and dependent variables was measured using the Spearman's Rank Correlation Coefficient (Spearman), a special case of the Pearson product moment correlation coefficient (Pearson) which measures the degree of association between two variables [5] [26], and its analysis is very efficient when dealing with Likert's ordinal information [33]. Spearman also evaluates how well relationships between (two) variables can be described using a monotonic (unchanged) function.

4. DATA ANALYSIS

4.1 Demographic Data

There were 34 valid responses out of 503 requests sent to financial auditors. This provided a response rate of 7%, which may be considered relatively small with limited potential for generalizing [18]. [31] experienced similar problems regarding their response rate in a study conducted in the U.S. about information security management effectiveness. Their response rate was only 4% (67 questionnaires received from 1,474 sent). The low response rate was supported by a further study concluding that the reasons for the non-responses were due to organizations' policies prohibiting sharing of their information, and a desire not to spend valuable working time. Such findings also explain the low response rate in the present study. For instance, various financial auditors replied that they could not respond due to information security policies in place at their organizations on disclosing information about clients. Others simply stated their intention of not completing the survey due to their current busy schedule. No follow-up requests were sent to address the low response rate within this research, as the research problem can be addressed satisfactorily with the information gathered from the survey.

This research is targeted at identifying a potential relationship between participation of IT auditors in financial audits and successful detection of manipulated financial information, which is considered independent of the sample size [18]. Because the respondents are competent and directly affected by this research, it is assumed that they provided a reliable and accurate assessment.

As for the respondents' personal background, 71% were males while 29% represented females. A 38% held Manager level positions, followed by a 29% for Seniors, 24% for Partners, and only a 9% for Staff. Financial auditors with 5 through 10, and over 20 years of experience represented the highest percentage (both with 29%). Most of their industry experience was in financial

services (47%) and the public sector and government (35%).

4.2 Analysis of Empirical Data

Likert scales, according to [9] and [17], fall within the ordinal level of measurement as the response categories have a rank order, but the intervals between values cannot be presumed equal. Consistent with the above, [13] indicates that to measure central tendency for ordinal data, where the numbers generally represent verbal statements, the mode should be employed as the arithmetical manipulations required to calculate the mean (and standard deviation) are inappropriate for ordinal data [9] [13]. For purposes of this research, Likert scales were treated as ordinal consistent with the definitions provided above.

The ordinal data collected was measured using non-parametric test-types of inferential statistics, such as Spearman, which is deemed appropriate when dealing with ordinal data [44], as parametric tests require interval and/or ratio type data [38] [13]. Spearman tests for order of relationships are very efficient when dealing with Likert's ordinal information. Spearman (often denoted by the Greek letter ρ or as r) evaluates how well relationships between (two) variables can be described using a monotonic function.

Spearman results from computation of the Pearson correlation coefficient between ranked variables [37] [34]. Spearman starts with converting raw scores (X_i , Y_i) into ranks (x_i , y_i). A difference is then computed between the ranks ($d_i = x_i - y_i$), and then squared. Assuming no computed ranks are tied or equal, the formula in Equation 1 is used, when d_i is the difference between ranks x_i , y_i ($d_i = x_i - y_i$), and n refers to the raw scores.

$$\rho = 1 - \frac{6 \sum d_i^2}{n(n^2 - 1)} \quad (1)$$

If, instead, tied ranks exist between two variables, an average of the tied ranks is computed. For instance, if two observations are equal for the third-highest rank, they would get a rank of 3.5 (the average of 3 and 4). Equation 2 shows the formula for calculating Spearman when ranks are equal [37].

$$r = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2 \sum_i (y_i - \bar{y})^2}} \quad (2)$$

Data from the questionnaire was downloaded into a Microsoft Excel spreadsheet and coded appropriately. The coding was established as follows: "Strongly Agree" as a value of 1, "Agree" as 2, "Neutral" as 3, "Disagree" as 4, and "Strongly Disagree" as 5. Each row of the spreadsheet represented a respondent while the columns were set as the two variables under study (i.e., "Inclusion of IT Auditors in Financial Audits" and "Identification of Manipulated Financial Information within IT Environments"). There were no blank responses, and only one negative-worded question. The response for the negative-worded question

was reversed for consistency purposes [44]. Responses were then segregated between the two variables.

Reliability of the questionnaire was established by testing for consistency and stability, as suggested by [44]. The Cronbach's alpha coefficient (Cronbach) is used for such purposes to indicate "how well the items in a set are positively correlated to one another" (p. 307). The closer the Cronbach is to 1, the higher the consistency and stability among the questions that make up each variable. Based on [19], a Cronbach of 0.70 or higher has also been widely accepted. The Cronbach computed for this study was 0.855 for the independent variable and 0.870 for the dependent variable, both indicating a high and acceptable level of reliability for each variable.

Then, the statistical mode was computed for each participant's response, as the measure of central tendency for ordinal-type data [3]. This provided an idea of how respondents reacted to the items in the survey. Once the statistical mode was calculated, consistent with the Spearman explanation above, ranks were obtained for each raw score. There were various tied ranks between the two variables. Therefore, an average of those tied/equal ranks was computed using the formula in Equation 2. The difference between the two ranks was then obtained, squared, and summed up, as required by the Spearman calculation. The formula in Equation 1 was then used to compute correlation. Next section will discuss and provide interpretations of the findings from the statistical analyses just described.

5. RESULTS AND DISCUSSION

The Cronbach values of 0.855 and 0.870 for the independent and dependent variables, respectively, indicate a high reliability. [44] suggests that reliabilities less than 0.60 are poor, while those over 0.80 represent good/high reliabilities. Reliabilities between 0.60 and 0.80, according to [19], are considered acceptable.

In terms of correlation, the formula in Equation 1 results in a Spearman of 0.614. From the Spearman's result, a positive correlation between the two variables is evident. In other words, there is a 0.614 significant correlation that when IT auditors are included in financial audits, manipulation of financial information will be successfully detected, thereby, substantiating the research hypothesis (H1). This means that for financial audit teams to detect if financial information has been manipulated or abused, IT auditors must become part of their teams. Non-involvement of IT auditors will increase audit risks which may be translated into opportunities for manipulation of financial information.

The findings above support the literature previously discussed (in Section 2) regarding the opportunities for manipulation, abuse, and/or misreport of financial data that may result from lack of involvement of IT auditors in financial audits. IT auditors have the required experience necessary for drawing accurate judgments when assessing risks and identifying error and irregularities within

organizations' financial information. More importantly, IT auditors are capable of selecting the best computer controls to fit the specific needs of organizations. Effective selection and testing of the most appropriate computer controls is a major step towards providing an adequate level of assurance that organizations' financial systems are adequately controlled and not subject to manipulation or abuse.

On the other hand, and also stated in the literature, financial auditors are not technical enough to perform the necessary IT procedures to conclude that financial systems are adequately controlled. Financial auditors are less likely to understand the control risks from IT environments and, therefore, may feel uncomfortable when performing computer-related audit procedures. In contrast, IT auditors have the technical knowledge to identify IT-related risks on financial systems, including areas sensitive to fraud or misbehavior by employees. The aforementioned is of significant help for organizations as fraud and manipulation of financial statement information continue its rapid ascending. The findings identified above also offer new insights for practice and research, both of which will be discussed next.

For practitioners, the findings of this research highlight the significance of participation of IT auditors in financial audits. When involved in financial audits, IT auditors perform procedures on financial systems to ensure the validity of transactions, accuracy and completion of reports, and to reduce the likelihood of financial misstatements. Furthermore, participation of IT auditors should be encouraged in order to identify instances where financial information has been manipulated.

As mentioned earlier, there are instances when IT auditors cannot become part of financial audits due to restrictions involving costs, availability, lack of IT skills experience, or simply because financial audit teams do not perceive such involvement as necessary. Although these instances exist and may be the only option in several audits, the findings from this study should prompt reconsideration of IT auditors' involvement among financial audits. Benefits from their inclusion should be compared to the costs that may be incurred as a result of no involvement.

Findings from this study also contribute to existing research by evidencing the importance of involving IT auditors in audit teams to prevent potential opportunities for manipulation, abuse, and/or misreport of financial data. The findings also support the arguments within the literature that auditors with specialized IT skills and experience are more likely to understand the organization's IT environment than financial auditors and, most importantly, identify the best set of computer controls to test IT processes over financial information.

There are some limitations within this research that are worth mentioning. First, the small sample size makes generalizing the results to a wider population difficult and complex [21] [43]. Second, the responses provided came from financial auditors and did not consider responses from IT auditors. Feedback from IT auditors can assist in

stressing the importance of their inclusion in financial audits. Third, the research did not investigate other effects, benefits, or disadvantages that inclusion of IT auditors may have (e.g., efficiencies in audit work, impact in audit costs, etc.).

In terms of opportunities for future work, results from this research may be extended to other geographic location, or to an entirely different sample to generalize the findings herein. Opportunities must also include refinement of the questions included within this study, or incorporation of additional ones that can improve the current investigation. Additionally, future research could examine why the use of IT auditors continues to be somewhat low, especially after results such as the findings from this research indicate the opposite. Future research could also examine if there is a general tendency to use more IT auditors in financial audit teams as organizations' IT environments become increasingly complex over time. Furthermore, future research could investigate whether the relationship between inclusion of IT auditors and detection of manipulated financial information has strengthened over time, and/or the effect(s) of a permanent inclusion of IT auditors in financial audit teams.

6. CONCLUSION

Studies continue to show harmful effects of unsuccessful IT implementations which result in opportunities for fraud and information security breaches. Surprisingly, IT auditors who can assist in detecting such opportunities are not being part of financial audit teams, or their use has been limited. This research provided an overview of the literature relevant to the question of whether involvement of IT auditors in financial audit teams assists the detection of manipulated financial data in organizations' IT environments. The study stressed that audit teams must comprise professionals with a balanced financial and IT-related understanding.

Literature regarding involvement of IT auditors was reviewed focusing on the need of adequate IT auditors' knowledge and experience when participating in financial audits. Literature was also reviewed in regards of manipulated financial information and its current rapid increase in organizations, followed by the importance of having IT auditors in financial audit teams to combat such increasing trend.

This research conducted survey analysis among financial auditors in order to investigate a potential relationship between inclusion of IT auditors in financial audit teams, and effective detection of manipulated financial information. The study revealed a clear linkage between the two, as evidenced by the positive relationship computed from the data analysis.

This research makes an important contribution in encouraging financial audit teams to reconsider whether client-related IT work should be overlooked and/or performed by financial auditors instead of utilizing the services of IT auditors. For some financial audit teams,

restrictions may still exist preventing such inclusion. Nonetheless, the risk of no inclusion must be measured and evaluated in terms of its impact in the overall audit of the organization.

REFERENCES

- [1] American Institute of Certified Public Accountants (AICPA). (2006b). Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement. Statement of Auditing Standards (SAS) No. 109. New York, NY: AICPA.
- [2] American Institute of Certified Public Accountants (AICPA). (2001). The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit. Statement of Auditing Standards (SAS) No. 94. New York, NY: AICPA.
- [3] Anderson, M., Banker, R. D., and Hu, N. (2002). Estimating the business value of investments in information technology. Proceedings of the Eighth Americas Conference on Information Systems, Dallas, TX, USA, 1195-1197.
- [4] Ashbaugh-Skaife, H., Collins, D. W., Kinney, W. R., and LaFond, R. (2008). The effect of SOX internal control deficiencies and their remediation on accrual quality. *The Accounting Review*, 83(1), 217-250.
- [5] Au, Y. A., Carpenter, D., Chen, X., and Clark, J. G. (2009). Virtual organizational learning in open source software development projects. *Information & Management*, 46(1), 9-15.
- [6] Bedard, J. C., and Biggs, S. (1991). Pattern recognition, hypotheses generation, and auditor performance in an analytical task. *The Accounting Review*, 66(3), 622-642.
- [7] Bedard, J. C., Graham, L., and Jackson, C. (2008). Archival evidence on detection and severity classification of Sarbanes-Oxley Section 404 internal control deficiencies. Working paper, Bentley University.
- [8] Bierstaker, J. L., Burnaby, P., and Thibodeau, J. (2001). The impact of information technology on the audit process: An assessment of the state of the art and implications for the future. *Managerial Auditing Journal*, 16(3), 159-164.
- [9] Blaikie, N. (2003). *Analyzing Quantitative Data*. London: Sage Publications.
- [10] Brazel, J. F., and Agoglia, C. P. (2007). An examination of auditor planning judgments in a complex accounting information system environment. *Contemporary Accounting Research*, 24(4), 1059-1083.
- [11] Carmichael, D. (2004). The PCAOB and the social responsibility of the independent auditor. *Accounting Horizons*, 18(2), 127-133.
- [12] Chai, S., Kim, M., and Rao, H. R. (2010). Firms' information security investment decisions: Stock

- market evidence of investors' behavior. *Decision Support Systems*, 50(4), 651-661.
- [13] Clegg, F. (1998). *Simple Statistics*. Cambridge: Cambridge University Press.
- [14] Curtis, B., Jenkins, J. G., Bedard, J., and Deis, D. R. (2009). Auditors' training and proficiency in information systems: A research synthesis. *Journal of Information Systems*, 23(1), 79-96.
- [15] Dawes, J. (2008). Do data characteristics change according to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales. *International Journal of Market Research*, 50(1), 61-77.
- [16] FBI, Federal Bureau of Investigation, Financial Crimes Report to the Public Fiscal Years 2007 through 2011, Department of Justice, United States, <http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011>
- [17] Goldstein, G., and Hersen, M. (1984). *Handbook of psychological assessment*. New York: Pergamon Press.
- [18] Hagen, J. M., Albrechtsen, E., and Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.
- [19] Hair, J. F. J., Anderson, R. E., Tatham, R. L., and Black, W. C. (1998). *Multivariate data analysis* (5th ed.). Upper Saddle River, New Jersey: Prentice Hall Inc.
- [20] Hall, J. A., and Liedtka, S. L. (2007). The Sarbanes-Oxley Act: Implications for large-scale IT outsourcing. *Communications of the ACM*, 50(3), 95-100.
- [21] Hartman, F., and Jugdev, K. (1998). Leadership undertow: Project manager fears and frustrations. *Proceedings of the 29th Annual Project Management Institute Seminars and Symposium*, Long Beach, USA.
- [22] Hoitash, R., Hoitash, U., and Bedard, J. C. (2008). Internal control quality and audit pricing under the Sarbanes-Oxley Act. *Auditing: A Journal of Practice & Theory*, 27(May), 105-126.
- [23] Huang, S. -M., Hung, W. -H., Yen, D. C., Chang, I. -C., and Jiang, D. (2010). Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems*, 50(4), 692-701.
- [24] Hunton, J. E., Wright, A. M., and Wright, S. (2004). Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? *Journal of Information Systems*, 18(2), 7-28.
- [25] Hwang, S. S., Shin, T., and Han, I. (2004). CRAS-CBR: Internal control risk assessment system using case-based reasoning. *Expert Systems*, 21(1), 22-33.
- [26] Ishioka, T. (2003). Evaluation of criteria for information retrieval, *Web Intelligence. Proceedings of the IEEE/WIC International Conference*.
- [27] Janvrin, D., Bierstaker, J., and Lowe, D. J. (2009). An investigation of factors influencing the use of computer-related audit procedures. *Journal of Information Systems*, 23(1), 97-118.
- [28] Johnson, P. E., Jamal, K., and Berryman, R. G. (1991). Effects of framing on auditor decisions. *Organization Behavior and Human Decision Processes*, 50(1), 75-105.
- [29] Kaplan, S. E., Moeckel, C and Williams, J. D. (1992). Auditors' hypothesis plausibility assessments in an analytical review setting. *Auditing: A Journal of Practice & Theory*, 11(Fall), 50-65.
- [30] Khalifa, G., Irani, Z., and Baldwin, L. P. (2000). IT evaluation methods: Drivers and consequences. *Proceedings of the Sixth Americas Conference on Information Systems*, Long Beach, CA, USA, 1142-1145.
- [31] Kotulic, A. G., and Clark, J. G. (2004). Why there aren't more information security research studies. *Information and Management*, 41(1), 607-697.
- [32] Leedy, P. D., and Ormrod, J. E. (2001). *Practical research* (7th ed.). Upper Saddle River, NJ: Merrill Prentice Hall.
- [33] Liu, Q., and Mintram, R. C., (2005). Preliminary Data Analysis Methods in Software Estimation. *Software Quality Journal*, 13(1), 91-115.
- [34] Maritz. J. S. (1981) *Distribution-Free Statistical Methods*. London: Chapman & Hall.
- [35] McAfee, A., and Brynjolfsson, E. (2008). Investing in the IT that makes a competitive difference. *Harvard Business Review*, 86(7/8), 98-107.
- [36] Musaji, Y. (2005). Sarbanes-Oxley and business process outsourcing risk. *Information Systems Control Journal*, 5(1), 47-50.
- [37] Myers, J. L., and Well, A. D. (2003). *Research Design and Statistical Analysis* (2nd ed.). Lawrence Erlbaum.
- [38] Pett, M. A. (1997). *Non-parametric Statistics for Health Care Research*. London: SAGE Publications.
- [39] Podsakoff, P. M., MacKenzie, S. B., Lee, J. -Y., and Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.
- [40] Ranganathan, C., and Brown, C. V. (2006). ERP investments and the market value of firms: Toward an understanding of influential ERP project variables. *Information Systems Research*, 17(2), 145-161.
- [41] Salkind, N. J. (2009). *Exploring research* (7th ed.). Upper Saddle River, NJ: Prentice Hall.
- [42] Schilit, H. M. (2002). *Financial Shenanigans*. New York, NY: McGraw-Hill.
- [43] Schmidt, R., Lyytinen, K., Keil, M., and Cule, P. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems*, 17(4), 5-36.

- [44] Sekaran, U. (2003). Research methods for business: A skill building approach (4th ed.). New York, NY: John Wiley & Sons, Inc.
- [45] Solomon, I., Shields, M. D., and Whittington, O. R. (1999). What do industry-specialist auditors know? *Journal of Accounting Research*, 37(1), 191-208.
- [46] Staehr, L. (2010). Understanding the role of managerial agency in achieving business benefits from ERP systems. *Information Systems Journal*, 20(3), 213-238.
- [47] Trivedi, T. (2007). 10 things to consider when offshoring operations. *Information Systems Control Journal*, 5(1), 1-2.
- [48] Tucker, G. (2001). IT and the audit. *Journal of Accountancy*, 192(3), 41-43.
- [49] Wright, S., and Wright, A. (1997). The effect of industry experience on hypothesis generation and audit planning decisions. *Behavioral Research in Accounting*, 9(1), 273-294.