IT Frauds and Audit Risks: Evidence of Improvements

Saeed Askary, Deakin University, Australia; E-mail: saskary@deakin.edu.au

ABSTRACT

This study examines whether frauds in Information Technology (IT) environment affects audit risk and quality. Information system technology dominates over almost every type of business and auditors should have enough knowledge and skills about those systems as part of their responsibilities to ensure about their client's internal control systems. Auditors should be able to examine the reliability of financial reporting process of those systems and provide audit opinion at the end. Thus, information systems audit, although integrated with the overall audit process and objectives, should finally facilitate for good corporate governance through providing quality audit report. This study uses data from Computer Crime and Security Survey (CCSS) 2006 to investigate the effects of IT risks on audit risks. Interestingly, the study find that the average improvements in audit of control risks is 49 percent, detection risk 46 percent, and inherent risk for as less as 25 percent. An overall improvement for auditor's risk is 41 percent in which it shows a considerable improvement.

Keywords: Audit Risks, IT Crimes, Frauds, Sarbanes-Oxley Act, Internal Control, IS Audit.

"Organizations are reporting a rise in fraud, responding with expanded fraud measures both reactive and preemptive, and planning further actions for the future." Richard H. Girgenti, National Partner in Charge KPMG Forensic (2003)

INTRODUCTION

The purpose of this study is to examine those information technology (IT) risks related to IT's attacks, crimes and frauds on the audit risk from 1999 until 2006. IT risks are key issues for auditors nowadays because of the vast impact of IT as well as the importance of information systems (I.Ss) on producing reliable data and valuable business information to various internal and external users. The impact of IT risk in form of IT crimes, frauds, misuse, attacks on audit risk is important in regard to audit quality and the credibility of financial reports. Moreover, it is important for corporate governance feat the auditor's opinion about how is the design and performance of the I.Ss in which are their direct responsibilities to be monitored and reviewed.

The reliability of information system is significantly depend on the design of the computerised internal controls systems and very critical for companies in achieving to their strategic goals, planning, as well as greater performance in term of high profitability. Information technology prevail over entities of all sizes and integrated with the internal control systems in many ways (Fukukawa, Mock, and Wright, 2006), and thus auditors should consider their due care and skill for understanding the internal control to perform during their audit engagements (ISA 315). Therefore, it is vital for auditors to understand those I.S. risks, frauds, crimes and IT attacks that causes many financial and non-financial damages to their clients. Then they should ensure designing those appropriate tests to ensure detecting the frauds, crimes, errors, and misstatements. A *priori* of the detrimental effects of the IT risks is that the diminishing quality of the I.Ss to generate relevant, reliable and timely reporting and increasing the audit risk. This implies that the IT threats must be identified and documented by auditors at one stage, and then the auditor's role is to analyse the threats along with test the other elements of the internal control system to find out the weakness or shortages to report them to managers in order to be improved and fixed.

The rest of the paper is organised in five sections. First, a discussion is provided about the audit risk and defines the auditors' responsibilities to understand and have enough knowledge and skills of their client IT environment and I.Ss. Then, IS risks are identified following up the methodology and results of the study. Conclusion section is presented at last.

IT AND AUDIT RISKS

According to O'Donnell and Moore (2005) "The pervasive use of systems in organisations and the increased emphasis on assurance of Information Technology (IT) processes has increased the need for accounting professionals with IT control knowledge and skills" (p.64). In addition, auditor should have enough competence including IT knowledge and skills, as required by Section 2 of the IES 8 to become a member of audit profession. This standard identifies two types of competence in form of *general* and *knowledge* contents. Paragraph 40 of the knowledge content requires "the knowledge content of the information technology subjects area should include, first, information technology systems for financial accounting and reporting, including relevant current issues and developments" and second, "frameworks for evaluating controls and assessing risks in accounting and reporting systems as appropriate for the audit of historical financial information" (p.11).

The latest Exposure Draft (ED) of the International Accounting Education Standards Board proposed as the International Education Practice Statement 2.1, *Information Technology for Professional Accountants.* In scope section of the practice statement, audit profession is categorised as "the accountant as assurance provider and evaluator". Paragraph 28 to 31 of the ED details all responsibilities of assurance provider and evaluator role in an IT environment and those required skills as depicted by the Appendix 4 of the ED. The appendix lists various IT tasks and related competence that IT auditors should have in three different areas. These are planning systems evaluation, evaluate systems and communicate results of evaluation and follow-up tasks. In plan systems evaluation, auditors are required to identify, analyse and evaluate risk factors and business issues affecting the IT assurance engagement or project and their implications.

In addition, auditors should also define level/frequency of systems errors, flaws and failures that are deemed significant or material in terms of audit risks. Gallegos (2002) by refer to well-know organisations such as the American Institute of Certified Public Accountants (AICPA), the US General Accounting Office (GAO), the Information Systems Audit and Control Association (ISACA)[1] and the Institute of Internal Auditors (IIA) also defined and listed twelve characters of the due professional care for IT auditors. They are peer review, audit conduct, communication, technical competence, judgment, business knowledge, training, certification, standards independence, continuous reassessment and high ethical standards. Therefore, authors are expected to comply with the characteristics and in case of any failure to detect any IT frauds, errors, misstatements, then this may be considered as an audit negligent, and may bear a legal action against the auditors.

According to Allen *et al.* (2006) strategic risk approach use "industry specialists appears to effectively promote understanding of a client's business risk" and they consider fraud risk as a "a particularly challenging task for auditors to perform" (p.161) . Traditional audit risk model, in which consist of inherent, control and detection risk, underpin the audits of financial statements (Blockdijk, 2004) and should be in the lowest acceptable level to increase the credibility of financial reports through lower level risk or risk free auditor's opinion. Thus, the lower audit risk, then the quality of audit opinion would be higher.

Many research have shown that inherent risk assessment has been interested on actual audit function (e.g. see Waller 1993, Mock and Wright 1993 and Elder and Allen 2003). Inherent risk related those susceptible account balances or transactions in which continued with different level of material misstatement, errors and frauds. Control risk is squarely related to internal control systems design and performance. Detection is the auditors' risk when they fail to detect any misstatement, errors, or fraud that affects fairness and truthfulness of financial statement reports in all material aspect. One exogenous factor influence audit risk is materiality and *a prior* in regard to risk evaluation is, those undetected immaterial risky balances or transactions would not affect the true and fairness of financial reports.

INFORMATION SYSTEMS' AUDIT

The ISACA extensively detailed the IS auditors' responsibilities and issued many comprehensive standards, guidelines and recommendations for this filed of auditing[2]. Based on ISACA, the purpose of IS audit is to review and provide feedback, assurance and suggestions and classifies major elements of IS audit into five broad areas such as physical and environmental review, system administration review, application software review, network security review, business continuity review, and data integrity review.

Notwithstanding I.S audit or general audit function, auditors should assess the integrity and robustness of internal control systems. The importance of internal controls generally is highlighted by the Sarbanes-Oxley Act in section 404, in which the Act requires organizations to select and implement a suitable internal control framework to strong corporate governance and reducing risk management by the accuracy, reliability, and integrity of an organization's transactional data. However, the significant role that information technology plays in design, efficiency and applicability of the internal controls need more attentions from auditors' perspectives to reduce IS audit risk as a point of quality audit opinion. Many IT environments' internal control framework such as COSO's *Internal Control—Integrated Framework* has become commonly used framework by many companies claim that the framework complies with Sarbanes-Oxley. However, according to Ernst & Young March 2005 survey of US listed foreign private issuers, almost half of the companies did not plan to conduct a separate and distinct fraud risk assessment of their internal controls in which required by SOX 404 to accomplished by 15 July 2006.

As a result of continuing efforts to define, assess, report on, and improve internal control systems recently five guidelines have been published by recognized professional bodies. These are the Information Systems Audit and Control Foundation issued COBIT (Control Objectives for Information and related Technology), the Institute of Internal Auditors Research Foundation by Systems Auditability and Control (SAC), the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework (COSO), and the American Institute of Certified Public Accountants issued the Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55), as amended by Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (SAS 78) (Janet L. Colbert, and Paul L. Bowen). Those reports reveal the importance of internal controls in an I.S audit environment particularly for risk assessment and internal controls structure.

Majority of professional accountants bodies (i.e. Big 4) provide the following services under Systems and Process Assurance (SPA) services[3] such as financial and operation applications, business process controls reviews, database security controls reviews, IT general controls reviews, infrastructure security reviews, third party assurance and opinion services, Sarbanes-Oxley readiness, process improvement and sustainability services, compliance with other regulatory requirements (e.g., Turnbull, Basel II, King), due diligence on systems and controls, pre and post-implementation systems reviews, project assurance services, data services (e.g., CAATs, data quality reviews), and computer security reviews.

DATA AND METHODOLOGY AND RESEARCH QUESTION

The study used the findings of Computer Crime and Security Survey (CCSS) 2006 due to the uniqueness of the survey in US. Respondents from corporations, government agencies, financial institutions, medical, and universities consist of 616 computer security practitioners. The survey measured the U.S dollar amount of losses by type of the computer crimes, security and frauds. Total losses for 2006 is US $52,494,290 mainly consisted of unauthorized access to information ($10,617,000), laptop or mobile hardware theft ($6,642,660), theft of proprietary information ($6,034,000), and financial fraud ($2,556,900) and other losses due to I.S risks are about $26,643,000. The main concentration has been devoted to CCSS's types and trends of the attacks, crimes, misuses, and fraud from 1999 to 2006 to answer this question:

Table 1. IT risks associated with the audit risk components

IT Frauds	Audit Risk Relevance
Theft of proprietary information	Control Risk
Insider abuse of net access	Control Risk
System penetration	Control Risk
Unauthorised access to information	Control Risk
Laptop/mobile theft	Control Risk
Telecom fraud	Detection Risk
Financial fraud	Detection Risk
Misuse of public web application	Inherent Risk
Virus	Inherent Risk
Abuse of Wireless network	Inherent Risk

Research Question : If audit risk is affected by IT risks, misuses and attacks and internal control systems, which is a great source for auditor to assess about control risks, are affected by the IT risk, then have improvements been taken places by the corporate entities since year 1999 to prevent those frauds?

In order to evaluate the effect of the IT risks, first a relationship between those IT risks should be established with audit risk components; that is, inherent risks, control risks, and detection risks. In order to have this relationship, Table 1 developed to summarise the IT risks which is adopted from figure 14 (p. 13) of the CCSS survey. For classification purpose of the IT risks, then theft of proprietary information, insider abuse of net access, system penetration, unauthorised access to information, and laptop mobile thefts are associated with the control risks and telecom and financial frauds are associated with the detection risk or auditor's risk. Misuse of public web application and virus and abuse of wireless network are considered to be inherent risks.

A trend analysis of the IS risks close to audit risks have been performed by looking at the data from 1999 till 2006. Then improved or declined percentages are measured to evidence of decrease or increase in overall audit risks.

RESULTS

Descriptive results of the CCSS survey shows that 21 percent[4] of respondents declared the experience of IT attacks, crimes and fraud risks that harmed the confidentiality, integrity or availability of network data and systems from as less as once to more than ten times. Various kinds of technologies used for the security purposes mainly were the anti-virus softwares (98 percent), Firewalls (95 percent) and Access Controls (93 percent). More interestingly, the respondents also used largely the computer security policies and procedures such system audit policy (51 percent), external network access control policies (75 percent), user access management(95 percent), media backup procedures (94 percent) and documented standard operating procedures(79 percent). Figure 1 graphically shows general improvements in IT risks as follows.

The figure generally demonstrates that a steady decrease in almost all of IT types of risks detected since 1999. Table 2 quantified all IT risks and their percentage of changes from the CCSS survey. There were, however, three areas in which average losses *increased.* Losses from laptop or mobile hardware theft increased from $19,562 per respondent in 2005 to $30,057 per respondent in 2006. Losses

IT Frauds and Audit Risks: Evidence of Improvements

Saeed Askary, Deakin University, Australia; E-mail: saskary@deakin.edu.au

ABSTRACT

This study examines whether frauds in Information Technology (IT) environment affects audit risk and quality. Information system technology dominates over almost every type of business and auditors should have enough knowledge and skills about those systems as part of their responsibilities to ensure about their client's internal control systems. Auditors should be able to examine the reliability of financial reporting process of those systems and provide audit opinion at the end. Thus, information systems audit, although integrated with the overall audit process and objectives, should finally facilitate for good corporate governance through providing quality audit report. This study uses data from Computer Crime and Security Survey (CCSS) 2006 to investigate the effects of IT risks on audit risks. Interestingly, the study find that the average improvements in audit of control risks is 49 percent, detection risk 46 percent, and inherent risk for as less as 25 percent. An overall improvement for auditor's risk is 41 percent in which it shows a considerable improvement.

Keywords: Audit Risks, IT Crimes, Frauds, Sarbanes-Oxley Act, Internal Control, IS Audit.

"Organizations are reporting a rise in fraud, responding with expanded fraud measures both reactive and preemptive, and planning further actions for the future." Richard H. Girgenti, National Partner in Charge KPMG Forensic (2003)

INTRODUCTION

The purpose of this study is to examine those information technology (IT) risks related to IT's attacks, crimes and frauds on the audit risk from 1999 until 2006. IT risks are key issues for auditors nowadays because of the vast impact of IT as well as the importance of information systems (I.Ss) on producing reliable data and valuable business information to various internal and external users. The impact of IT risk in form of IT crimes, frauds, misuse, attacks on audit risk is important in regard to audit quality and the credibility of financial reports. Moreover, it is important for corporate governance feat the auditor's opinion about how is the design and performance of the I.Ss in which are their direct responsibilities to be monitored and reviewed.

The reliability of information system is significantly depend on the design of the computerised internal controls systems and very critical for companies in achieving to their strategic goals, planning, as well as greater performance in term of high profitability. Information technology prevail over entities of all sizes and integrated with the internal control systems in many ways (Fukukawa, Mock, and Wright, 2006), and thus auditors should consider their due care and skill for understanding the internal control to perform during their audit engagements (ISA 315). Therefore, it is vital for auditors to understand those I.S. risks, frauds, crimes and IT attacks that causes many financial and non-financial damages to their clients. Then they should ensure designing those appropriate tests to ensure detecting the frauds, crimes, errors, and misstatements. A *priori* of the detrimental effects of the IT risks is that the diminishing quality of the I.Ss to generate relevant, reliable and timely reporting and increasing the audit risk. This implies that the IT threats must be identified and documented by auditors at one stage, and then the auditor's role is to analyse the threats along with test the other elements of the internal control system to find out the weakness or shortages to report them to managers in order to be improved and fixed.

The rest of the paper is organised in five sections. First, a discussion is provided about the audit risk and defines the auditors' responsibilities to understand and have enough knowledge and skills of their client IT environment and I.Ss. Then, IS risks are identified following up the methodology and results of the study. Conclusion section is presented at last.

IT AND AUDIT RISKS

According to O'Donnell and Moore (2005) "The pervasive use of systems in organisations and the increased emphasis on assurance of Information Technology (IT) processes has increased the need for accounting professionals with IT control knowledge and skills" (p.64). In addition, auditor should have enough competence including IT knowledge and skills, as required by Section 2 of the IES 8 to become a member of audit profession. This standard identifies two types of competence in form of *general* and *knowledge* contents. Paragraph 40 of the knowledge content requires "the knowledge content of the information technology subjects area should include, first, information technology systems for financial accounting and reporting, including relevant current issues and developments" and second, "frameworks for evaluating controls and assessing risks in accounting and reporting systems as appropriate for the audit of historical financial information" (p.11).

The latest Exposure Draft (ED) of the International Accounting Education Standards Board proposed as the International Education Practice Statement 2.1, *Information Technology for Professional Accountants.* In scope section of the practice statement, audit profession is categorised as "the accountant as assurance provider and evaluator". Paragraph 28 to 31 of the ED details all responsibilities of assurance provider and evaluator role in an IT environment and those required skills as depicted by the Appendix 4 of the ED. The appendix lists various IT tasks and related competence that IT auditors should have in three different areas. These are planning systems evaluation, evaluate systems and communicate results of evaluation and follow-up tasks. In plan systems evaluation, auditors are required to identify, analyse and evaluate risk factors and business issues affecting the IT assurance engagement or project and their implications.

In addition, auditors should also define level/frequency of systems errors, flaws and failures that are deemed significant or material in terms of audit risks. Gallegos (2002) by refer to well-know organisations such as the American Institute of Certified Public Accountants (AICPA), the US General Accounting Office (GAO), the Information Systems Audit and Control Association (ISACA)[1] and the Institute of Internal Auditors (IIA) also defined and listed twelve characters of the due professional care for IT auditors. They are peer review, audit conduct, communication, technical competence, judgment, business knowledge, training, certification, standards independence, continuous reassessment and high ethical standards. Therefore, authors are expected to comply with the characteristics and in case of any failure to detect any IT frauds, errors, misstatements, then this may be considered as an audit negligent, and may bear a legal action against the auditors.

According to Allen *et al.* (2006) strategic risk approach use "industry specialists appears to effectively promote understanding of a client's business risk" and they consider fraud risk as a "a particularly challenging task for auditors to perform" (p.161) . Traditional audit risk model, in which consist of inherent, control and detection risk, underpin the audits of financial statements (Blockdijk, 2004) and should be in the lowest acceptable level to increase the credibility of financial reports through lower level risk or risk free auditor's opinion. Thus, the lower audit risk, then the quality of audit opinion would be higher.

Many research have shown that inherent risk assessment has been interested on actual audit function (e.g. see Waller 1993, Mock and Wright 1993 and Elder and Allen 2003). Inherent risk related those susceptible account balances or transactions in which continued with different level of material misstatement, errors and frauds. Control risk is squarely related to internal control systems design and performance. Detection is the auditors' risk when they fail to detect any misstatement, errors, or fraud that affects fairness and truthfulness of financial statement reports in all material aspect. One exogenous factor influence audit risk is materiality and *a prior* in regard to risk evaluation is, those undetected immaterial risky balances or transactions would not affect the true and fairness of financial reports.

INFORMATION SYSTEMS' AUDIT

The ISACA extensively detailed the IS auditors' responsibilities and issued many comprehensive standards, guidelines and recommendations for this filed of auditing[2]. Based on ISACA, the purpose of IS audit is to review and provide feedback, assurance and suggestions and classifies major elements of IS audit into five broad areas such as physical and environmental review, system administration review, application software review, network security review, business continuity review, and data integrity review.

Notwithstanding I.S audit or general audit function, auditors should assess the integrity and robustness of internal control systems. The importance of internal controls generally is highlighted by the Sarbanes-Oxley Act in section 404, in which the Act requires organizations to select and implement a suitable internal control framework to strong corporate governance and reducing risk management by the accuracy, reliability, and integrity of an organization's transactional data. However, the significant role that information technology plays in design, efficiency and applicability of the internal controls need more attentions from auditors' perspectives to reduce IS audit risk as a point of quality audit opinion. Many IT environments' internal control framework such as COSO's *Internal Control—Integrated Framework* has become commonly used framework by many companies claim that the framework complies with Sarbanes-Oxley. However, according to Ernst & Young March 2005 survey of US listed foreign private issuers, almost half of the companies did not plan to conduct a separate and distinct fraud risk assessment of their internal controls in which required by SOX 404 to accomplished by 15 July 2006.

As a result of continuing efforts to define, assess, report on, and improve internal control systems recently five guidelines have been published by recognized professional bodies. These are the Information Systems Audit and Control Foundation issued COBIT (Control Objectives for Information and related Technology), the Institute of Internal Auditors Research Foundation by Systems Auditability and Control (SAC), the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework (COSO), and the American Institute of Certified Public Accountants issued the Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55), as amended by Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (SAS 78) (Janet L. Colbert, and Paul L. Bowen). Those reports reveal the importance of internal controls in an I.S audit environment particularly for risk assessment and internal controls structure.

Majority of professional accountants bodies (i.e. Big 4) provide the following services under Systems and Process Assurance (SPA) services[3] such as financial and operation applications, business process controls reviews, database security controls reviews, IT general controls reviews, infrastructure security reviews, third party assurance and opinion services, Sarbanes-Oxley readiness, process improvement and sustainability services, compliance with other regulatory requirements (e.g., Turnbull, Basel II, King), due diligence on systems and controls, pre and post-implementation systems reviews, project assurance services, data services (e.g., CAATs, data quality reviews), and computer security reviews.

DATA AND METHODOLOGY AND RESEARCH QUESTION

The study used the findings of Computer Crime and Security Survey (CCSS) 2006 due to the uniqueness of the survey in US. Respondents from corporations, government agencies, financial institutions, medical, and universities consist of 616 computer security practitioners. The survey measured the U.S dollar amount of losses by type of the computer crimes, security and frauds. Total losses for 2006 is US $52,494,290 mainly consisted of unauthorized access to information ($10,617,000), laptop or mobile hardware theft ($6,642,660), theft of proprietary information ($6,034,000), and financial fraud ($2,556,900) and other losses due to I.S risks are about $26,643,000. The main concentration has been devoted to CCSS's types and trends of the attacks, crimes, misuses, and fraud from 1999 to 2006 to answer this question:

Table 1. IT risks associated with the audit risk components

IT Frauds	Audit Risk Relevance
Theft of proprietary information	Control Risk
Insider abuse of net access	Control Risk
System penetration	Control Risk
Unauthorised access to information	Control Risk
Laptop/mobile theft	Control Risk
Telecom fraud	Detection Risk
Financial fraud	Detection Risk
Misuse of public web application	Inherent Risk
Virus	Inherent Risk
Abuse of Wireless network	Inherent Risk

Research Question : If audit risk is affected by IT risks, misuses and attacks and internal control systems, which is a great source for auditor to assess about control risks, are affected by the IT risk, then have improvements been taken places by the corporate entities since year 1999 to prevent those frauds?

In order to evaluate the effect of the IT risks, first a relationship between those IT risks should be established with audit risk components; that is, inherent risks, control risks, and detection risks. In order to have this relationship, Table 1 developed to summarise the IT risks which is adopted from figure 14 (p. 13) of the CCSS survey. For classification purpose of the IT risks, then theft of proprietary information, insider abuse of net access, system penetration, unauthorised access to information, and laptop mobile thefts are associated with the control risks and telecom and financial frauds are associated with the detection risk or auditor's risk. Misuse of public web application and virus and abuse of wireless network are considered to be inherent risks.

A trend analysis of the IS risks close to audit risks have been performed by looking at the data from 1999 till 2006. Then improved or declined percentages are measured to evidence of decrease or increase in overall audit risks.

RESULTS

Descriptive results of the CCSS survey shows that 21 percent[4] of respondents declared the experience of IT attacks, crimes and fraud risks that harmed the confidentiality, integrity or availability of network data and systems from as less as once to more than ten times. Various kinds of technologies used for the security purposes mainly were the anti-virus softwares (98 percent), Firewalls (95 percent) and Access Controls (93 percent). More interestingly, the respondents also used largely the computer security policies and procedures such system audit policy (51 percent), external network access control policies (75 percent), user access management(95 percent), media backup procedures (94 percent) and documented standard operating procedures(79 percent). Figure 1 graphically shows general improvements in IT risks as follows.

The figure generally demonstrates that a steady decrease in almost all of IT types of risks detected since 1999. Table 2 quantified all IT risks and their percentage of changes from the CCSS survey. There were, however, three areas in which average losses *increased.* Losses from laptop or mobile hardware theft increased from $19,562 per respondent in 2005 to $30,057 per respondent in 2006. Losses