www.irmbrjournal.com June 2014
International Review of Management and Business Research Vol. 3 Issue.2

Information Security for Organizations and Accounting Information Systems

A Jordan Banking Sector Case

SHAMSI S. BAWANEH
Department of Accounting King Talal School for Business and Technology
Princess Sumaya University for Technology
P.O. Box 1438 Amman 11941 Jordan.
Email: s.bawaneh@psut.edu.jo
Tel: (+962 77 778 4947); (+962 79 665 7050)
Fax No.: (+962 6 534 7295)

Abstract

This research examines three types of information security and control procedures for organizations that are expected to be used within Accounting Information Systems (AIS): security and general control for organizations; security and general control for Information Technology (IT), and application controls for transaction processing. In practice, this study found that banks, to be able to protect themselves against computer fraud, formulate control procedures relate to input controls, processing controls, output controls, and physical security. Furthermore, banks and accountants in their practice adapted several methods for thwarting (mitigating) computer crimes, abuses, and fraud as follows: Enlist top-management support; Increase employee awareness and education[1]; Assess security measures and protects passwords[2]; Implement controls which based on the believe that most computer crimes and abuse succeed because of the absence of control rather than the failure of control. The study found that the solution to the computer-security problems of most banks is straightforward: design and implement control. This means that accountants install control procedures to deter computer crimes, and managers enforce them, and both internal and external auditors test them. Furthermore, the study found that no bank Employ forensic accountants in the normal situation. Top managers in many banks explain that when a bank suspects an ongoing computer crime or fraud, it can hire forensic accountants to investigate its problems, document findings, and make recommendations. Accountants may use specialized software tools to help them perform their tasks[3]. Good security for banks starts with a clear disaster recovery plan and a solid security policy which are not applied and many banks are not conducting a risk assessment procedure. Probably the best security investment in Jordanian banks is user training: training individual users on data recovery and ways to defeat social engineering.

Key Words: *Information Security, Information Technology, Control Procedures, Accounting Information Systems, Internet, Computer Abuse, Fraud, Forensic Accounting, Corporate Governance, Financial Institutions, Jordan.*

[1] KPMG Forensic Integrity Survey 2005-2006, http://www.us.kpmg.com/news/index.asp?cid=2051
[2] For recommended steps for safeguarding personal computers, see Bagranoff *et al.*, 2010, p. 328.
[3] For example, Audit Command Language (ACL) for auditing tasks, and EnCase for file copying, custody documentation, and other forensic activities.

Introduction

Business and government have always been concerned with physical and information security. They have protected physical assets with locks, barriers, guards, and they have also guarded their plans and information with coding systems since organized societies began. What has changed in the last 50 years is the introduction of computers and the Internet and their securities, which are the focus of this research.

The rise of the Internet has completely redefined the nature of information security. Now companies face global threats to their networks, and, more importantly, to their data. The number of Internet security incidents reported to the Computer Emergency Response Team (CERT)[4] doubled every year up until 2003, when CERT stopped keeping records because there were so many incidents that it was no longer meaningful to keep track (Dennis & Durcikova, 2012).

Developing a secure network means developing controls. Controls are software, hardware, rules, or procedures that reduce or eliminate the threats to network security. Controls prevent *which mitigate or stop a person from acting or an even from occurring*, detect *which reveal or discover unwanted events*, and/or correct *which remedy an unwanted event or an intrusion*, whatever might happen to the organization because of threats facing its computer- based systems[5].

Information technology (IT), properly used, can have enormous benefits for individuals, organizations, and entire societies. So far, we have seen diverse ways in which IT has made businesses more productive, efficient, and responsive to consumers. Unfortunately, information technologies can also be misused, often with devastating consequences. In fact, the misuse of information technologies has come to the forefront of any discussion of IT (Rainer & Cegielski, 2013). For example, a research firm[6] found that in 2010 each security breach cost organizations an average of $6.75 million and concluded that employee negligence caused many of the data breaches. This finding confirms that organizational employees are a weak link in information security. It is therefore very important for us to learn about information security, this is one of the motivations of this research, so that we will be better prepared when we enter the workforce and conduct our task.

As we know, IT is pervasive, as are the networks that may be used to access information anytime, anywhere. One of the primary challenges associated with all this connectivity is security which is the focus of this research. The question now, how do we protect sensitive data and information that is stored or transferred from one device to another? The answer is that organizations must have the appropriate security and control procedures in place which is examine by this research. Although no organization can be 100% confident that its assets are protected, the goal of this research is to obtain a reasonable level of assurance.
Security can be defined as the degree of protection against criminal activity, danger, damage, and /or loss. Following this broad definition, information security refers to all of the process and policies designed to protect an organization's information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Organizations collect huge amounts of information and employ numerous information systems that are subject to myriad threats. A threat to an information resource is any danger to which a system may be exposed. The exposure of an information resource is the harm, loss, or

[4] CERT was established by the U.S. Department of defense at Carnegie Mellon University with a mission to work with the Internet community to respond to computer security problems, raise awareness of computer security issues, and prevent security breaches. CERT maintains a Web site on security at www.cert.org. Another site for security information is www.infosyssec.net.

[5] For a more basic control principles of a secure network see, Dennis & Durcikova 2012, p. 346.

[6] www.ponemon.org

damage that can result if a threat compromises that resource. An information resource's vulnerability is the possibility that the system will be harmed by a threat. Today, five key factors are contributing to the increasing vulnerability of organizational information resources, making it much more difficult to secure them: the first factor is the evolution of the IT resource from mainframe-only today's complex, interconnected, interdependent, wirelessly networked business environment. The second factor reflects the fact that modern computers and storage devices continue to become smaller, faster, cheaper, and more portable, with greater storage capacity. The third factor is that the computing skills necessary to be a hacker are decreasing. The fourth factor is that international organized crime is taking over cybercrime. The fifth, and final, factor is lack of management support (Rainer & Cegielski 2013, pp. 83-84).

The remainder of this study is divided into five sections. The next section presents a theoretical background of this study. Section three provides a literature review. The fourth section presents the research methodology and describes the research method adapted. The fifth section presents the results and the analysis followed by the conclusion section.

Theoretical Background

Information Technology (IT) refers to the hardware and software used in computerized information systems and has been a major force in shaping our current society. Such technology influences our lives in many personal ways. In this information age, for example, fewer workers actually make products while more of them produce, analyze, manipulate, and distribute information about business activities. These individuals are often called "Knowledge workers" (see, Thottam, 2004). Companies find that their success or failure is often dependent on the uses or misuses of the information that knowledge workers manage.

Consistent with this view, Bagranoff *et al.* (2005) viewed accountants as knowledge workers and the information age has an important implication for accounting. Because their role has been, in part, to communicate[7] accurate and relevant financial information to parties interested in how their organizations are performing, accountants have always been in the "information business".

In a computerized system, the collection, recording and transmitting accounting data are done automatically or by giving the command to process. Also, financial reports are generated based on an instruction given to the computer which is actually a group of hardware components that work together with software to perform a specific task which enable an Accounting Information System (AIS) to fulfill its functions in any organization.

This study expected that to be able to give the accountants the scope of knowledge needed in real-life situation, the study of IT should be integrated as far as possible in the study of accounting, which allow the accountants to evaluate the performance of information systems in an accurate and timely manner. Therefore, the technology should be studied from the perspective of their usefulness and application to

[7] In Statement of Financial Accounting Concepts No.2, the Financial Accounting Standards Board defines Accounting as being an Information System. It also that the primary objective of Accounting is to provide information useful to decision marks. Therefore, it is not surprising that the Accounting Education Change Commission recommended that the Accounting curriculum should emphasize that Accounting is an information identification, development, measurement, and communication process. The commission suggested that the Accounting curriculum should be designed to provide students with a solid understanding of three essential concepts: (1) the use of information in decision making, (2) the nature, design, use, and implementation of AIS, and financial information reporting (Romney & Steinbart, 2000 pp 4-5).

business situation and should not be seen as an end in itself. The business press frequently reports the many ways in which IT is profoundly changing the way that accounting and many other business activities are performed. Because this impact is likely to continue, the study focuses on understanding how IT can be used to improve the performance of AIS and then the quality of accounting control system in general and specifically, this research will focus on specific security and control procedures that organizations may use at three different control levels. The highest level takes the perspective of "enterprise-wide," which encourages organizations to use resources efficiently. At the next level, the research discusses general control for information technology that the organization uses. Application controls are the third level of controls which are designed to protect transaction processing.

Enterprise – Level Controls

In this highest level, security and control procedures begin with a security policy which is a comprehensive plan that helps protect an enterprise from both internal and external threats and should comply with ISO 17799, the international information security standards that establish information security best practices[8]. This standard includes ten primary sections: security policy, system access control, computer and operations management, system development and maintenance, physical and environmental security, compliance, personal security, security organization, asset classification and control, and business continuity management. A current trend in security practice is to merge physical security and logical security across an organization. Physical security refers to any measures that an organization uses to protect its facilities, resources, or its proprietary data that are stored on physical media. And logical security uses technology to limit access to the organization's systems and information to only authorized individuals. In addition to these security procedures, management must have control over the human resources and data resources of the firm (For more details, see Bagranoff, *et al.*, 2010, pp. 381-390). These organization- level controls are so important because they often have a pervasive impact on many other controls, such as IT general controls and application- level controls.

In the light of the fact that natural and man-made disasters are becoming more frequent, firms and organizations of all sizes must now become more intentional about developing and testing a disaster recovery plan in support of general controls. Also, according to Rainer & Cegielski (2013) a solid backup plan is critical to information security and this process for small business is more important as any loss of data could mean lost customers and lost revenue.

Information Technology Controls

The information technology general controls are controls that are embedded in IT processes and are applied to all IT service activities. The major objectives of an organization's IT controls are to provide reasonable assurance that (1) development of , and change to, computer programs are authorized, tested, and approved before their usage, and (2) access to programs and data is granted only to authorized users to increase the likelihood that processed accounting data are accurate and complete. These controls are critical for reliance on application controls.

Application Controls

The purpose of application controls is to prevent, detect, and correct errors and irregularities in processing transactions. Application controls are those controls that are embedded in business process applications. The three major stages of data processing work are accumulating the input data, processing the data, and

[8] http://iso-17799.com

reporting the processed data in some form of output (e.g., a performance report). There are various application control procedures for AISs based on these three stages. First, the research examines application controls over data input (called input controls). Next, identifies application controls that are intended to protect the processing of data (called processing controls), and finally, surveys application controls related to data output (called output controls).

Literature Review

In automated accounting systems, IT serves as a platform on which other system components in part rely. According to Bagranoff *et al.* (2005) AIS view as a set of five interacting components: hardware, software, data, people, and procedures. Computer hardware is probably the most tangible element in this set, but "hardware" is only one piece of the pie. Computer hardware must work together with the other system components to accomplish data processing tasks. Without computer software, for example, the hardware would stand idle. Without data to process, both the hardware and the software would be useless. Without procedures, accounting data could not be gathered accurately or distributed properly. And finally, without people, it is doubtful that the rest of the system could operate for long or be of much use.

Researchers (Anderson, 2002; Huber, 2004) make clear that IT and accounting systems are intimately related, and a computer system must interact with all the other system components to create a working AIS[9]. Giddens (1984) explains that using and developing IT in accounting firms is considered an essential element through which such firms can strongly establish themselves and improve their productivity.

The information age and the IT that created it are influencing all areas of accounting, including financial and managerial accounting, auditing, and taxation. With respect to financial accounting, critics contend that periodic, audited financial statements are less relevant in the information age. The accounting profession has responded by studying the needs of financial information users and improving the relevance of accounting information. Managerial accounting is also developing new costing approaches such as activity-based costing systems, new performance measurement approaches such as the balanced scorecard (Kaplan & Norton, 2001), and new IT to help managers make more informed business decisions (Zeller *et al.*, 2001). Auditing practice is expanding to include a variety of new assurance services, and the nature of the audit has also shifted (AICPA/CICA, 1999). Finally, the availability of tax software and extensive tax databases influences both tax preparation and tax planning.

Therefore, the use of computer in the college classroom has become so commonplace that on most campuses, it is difficult to find a classroom that does not have at least an instructor computer workstation connected to a projector (Guthrie & Carlin, 2004). Also, it is likely to affect the way accountants will work in the future. IT will become even more important to accountants as AIS continue to incorporate technological advances in their designs, and also as this technology becomes more important to their daily professional and personal tasks. These reasons became major factors to conduct this study. Therefore, this view consists with Bagranoff *et al.* view (2005) that there are many reasons to study AIS and to recognize the importance of IT to it.

The importance of IT in developing of AIS

Before recognizing AIS we have to understand the terms data and information which are the raw material for an AIS and both are some of an organization's most valuable assets according to Romney & Steinbart

[9] Others researchers present six reasons to show that IT is important to accountants and must be compatible with, and support, the other components of an AIS (for details, see Bagranoff et al, 2005).

(2003). Data refers to any and all of the facts that are collected, stored, and processed by an information system[10]. Once data have been collected, it is the job of the AIS to transform the facts into useful information so they can be used to make decisions[11].

The study of AISs is, in large part, the study of the application of IT to accounting systems. We begin by answering the question, "What are AISs?" and then look at some advantages of developing the characteristics of AIS which affected by IT.

Many researches (Bagranoff *et al.*, 2005; Romney & Steinbart, 2003; Moscove & Simkin, 1984) believed that we cannot define AIS by its size, but it is better to define it by what it does. Bagranoff *et al.* (2005) define AIS "is a collection of data and processing procedures that creates needed information for its users" and suggest that AISs stand at the crossroads of two disciplines: accounting and information systems. In the same track Moscove & Simkin (1984) define AIS as "an organizational component which accumulates, classifies, processes, analyzes, and communicates relevant financial-oriented, decision-making information to a company's external parties and internal parties." (pp. 6-7).

We conclude from these definitions that, it is convenient to conceptualize AIS as a set of components that collect accounting data, record it, store it for future uses, and process it for end users[12]. Today, however, AISs are concerned with nonfinancial as well as financial data and information because that many of the end users of the information of an AIS are not accountants, but include customers, investors, suppliers, financial analysts, and government agencies. Thus, the present definition of AIS as an enterprise wide system views accounting as an organization's primary producer and distributor of many different types of information.

Consistent with previous definitions Romney & Steinbart (2003) argued that AIS consists of five components: people, procedures, data, software, and information technology infrastructure. Together, these five components enable AIS to fulfill three important functions in any organization:

- Collecting and storing data about the activities performed by the organization,
- Transforming data into information that is useful for making decisions that enable management to plan, execute, and control activities,
- Providing adequate controls to safeguard the organization's assets, including its data, to ensure that the data are available when needed and are accurate and reliable.

Thus, the study of AISs is viewed as the study of computerized accounting systems. Computerized accounting systems, in the information age, perform many of the tasks once performed by traditional manual systems- for example, collecting, processing, storing, transforming, and distributing both financial and non-financial information for planning, decision-making, and control purposes.
Therefore, most accounting transactions, which are done automatically or by given the command to the computer, are processed in a three-phase operation called input-processing-output cycle. The starting point

[10] Romney and Steinbart (2003) show three kinds of data need to be collected for any activity: facts about the event itself, the resources affected by the event, and the agents who participated in that event (p.9).

[11] To make information meaningful and useful for decision making, Romney and Steinbart, (2003) intended that it must have the following characteristics: relevant, reliable, complete, timely, understandable, and verifiable.

[12] So that, it is useful view AIS as a collection of hardware, software, data, people, and procedures that must all work together to accomplish processing tasks.

of the input-processing-output cycle –especially when organizations process accounting transactions- is input which is a record of business activities. Thus, even where the amount of data is small, computerized AISs require input methods and procedures that ensure complete, accurate, timely, and cost-effective ways of gathering and inputting accounting data. The starting point for collecting accounting data in most AISs is a source documents. A source document is a piece of paper or an electronic form that records a business activity such as the purchase or sale of goods. Therefore, in order to process source-document data electronically, the data must first be transcribed into machine-readable media, where most AIS designers prefer data-capturing methods that gather data that are already in machine-readable formats, because electronic source documents eliminate many errors that are introduced by human input. Therefore, computerized AISs make extensive use of source documents. Also, source documents help manage the flow of accounting data in several ways (Bagranoff *et al.*, 2005)[13].

Many devices enable AISs to capture data[14] that are already in machine-readable formats, and to store and archive data on media[15] that permanently maintain its accuracy and integrity, yet permit the system to access and modify this information quickly and easily.

A well-designed computerized AIS can add value to the organization by: improving the quality and reducing the costs of products or services by reducing the amount of wasted materials, improving efficiency of operations by providing more timely information, improved decision making by providing accurate information in a timely manner, and sharing of knowledge by providing competitive advantages.
The information produced by well-designed computerized AIS can improve decision making in several ways. First, it identifies situations requiring management action. Second, by reducing uncertainty, accounting information provides a basis for choosing among alternative actions. Third, information about the results of previous decisions provides valuable feedback that can be used to improve future decisions (for details, see Romney & Steinbart, 2003).

Therefore, the advances in IT will permit AIS to create more information. Nevertheless, although more information is often better, this is only true to a point. There are limits to the amount of information that the human mind can effectively absorb and process. Information overload occurs when those limits are passed. Information overload is costly, because decision-making quality declines while the costs of providing that information increase. Thus, information overload reduces the value of information. Consequently, information systems designers must consider how advances in IT can help decision makers more effectively filter and condense information, thereby avoiding information overload.

These arguments allow us to raise this question: how AISs operate properly and record accounting data accurately? Documentation explains how AISs operate and is therefore a vital part of any accounting system. For example, documentation describes the tasks for recording accounting data, the procedures that users must perform to operate computer applications, the processing steps that computer systems follow, and the logical and physical flows of accounting data through the system (Bagranoff *et al.*, 2005)[16].

[13] First, they dictate the kinds of data to be collected and help ensure legibility, consistency, and accuracy in recording data. Second, they encourage the completeness of accounting data because these source documents clearly enumerate the information required. Third, they serve as distributors of information for individuals or departments. Finally, source documents help to establish the authenticity of accounting of accounting data.

[14] POS devices, MIRC readers, OCR readers, and magnetic-strip readers

[15] Magnetic (hard) disks, floppy disks, CD- ROMs, DVD disks, and USB flash disks

[16] There are seven reasons to document AIS:
(1) to explain how the system works, (2) to train others, (3) to help develops design new systems, (4) to control system development and maintenance costs, (5) to standardize communications among system

Therefore, documentation includes all the flowcharts, narratives, and other written communications that describe the inputs, processing, and outputs of AIS. By using IT, these flowcharts pictorially represent data paths in compact formats and therefore save pages of narrative description and make better communications.

The information which are created and documented by computerized AISs will be used by interested users in different locations. According to Moscove & Simkin (1984) in their definition for AISs insisted that AIS communicates financial information to both company's external and internal parties. In this situation, IT will be very helpful in transmitting accounting data and information to various locations, because, data communication which refers to transmitting data to and from remote locations, enable AISs to transmit accounting data over local and wide area networks. Many accounting applications use data communications in normal business operations. For example, banking systems enable individual offices to transmit deposit and withdrawal information to centralized computer locations. Therefore, accountants must understand data communication concepts because so many AISs use them and also because so many clients acquire AISs that depend on data transmissions. Many AISs now use LANs or WANs for e-mail, sharing computer resources, saving software costs, gathering input data, or distributing outputs. Wi-Fi technology[17] of the future will significantly increase the ability of accountants to be mobile, yet connected to their offices as well as to their clients (Malik, 2003).

Furthermore, the connection between accounting and computer crimes and fraud is both straightforward and important (Bagranoff *et al.*, 2010). Managers, accountants, and investors all use computerized financial accounting information to control valuable resources, authenticate accounting transactions, and make investment decisions. But the effectiveness of these activities can be lost if the underlying information is wrong, incomplete, or seriously compromised. This is why digital information in itself is a valuable asset that must be protected. The more managers and accountants know about computer crimes and fraud, the better they can assess risks and implement control to protect organizational assets.

Although the terms "computer crime" and "computer abuse" seem to describe the same problem, there is a subtle difference between them[18]. The type of computer crime with which most professional accountants are familiar is financial fraud. Statement on Auditing Standards No. 99 identifies two types of fraud; (1) fraudulent financial reporting and (2) misappropriation of assets[19]. Although data on computer crimes and fraud are limited, at least three reputable organizations conduct surveys that help us understand the breadth and depth of these crimes[20].

In addition to the typical accounting services rendered by accountants, the profession is rapidly moving into other value-added services known as fraud investigation (or litigation support) or the broader, more

designers, (6) to provide information to auditors, and (7) to document a business's processes (for details, see Bagranoff et al 2005).

[10] Wi-Fi is the ability to transmit voice- grade signals or digital data over wireless communication channels. Wi-Fi application has two dimensions: connectivity and mobility.

[18] **Computer crime** involves the manipulation of a computer or computer data, by whatever method, to dishonestly obtain money, property, or some other advantage of value, or cause a loss. In contrast, **computer abuse** means the unauthorized use of, or access to, a computer for purposes contrary to the wishes of the computer's owner. Vogon International website: www.vogon-international.co.uk.

[19] Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA 2003)

[20] First, the Computer Security Institute (CSI) survey Second, KPMG survey, and third the Association of Certified Fraud Examiners (ACFE) survey

comprehensive term of forensic accounting. The terms forensic accounting and litigation support generally imply the use of accounting in a court of law. Thus, the services of an accountant in a fraud investigation or court case are often referred to as forensic accounting or litigation support services[21].

Fraud is a major problem for most organizations (Albrecht *et al.*, 1995). Stories about fraud often appear in newspapers and business periodicals. A review of such articles reveals that fraud is not perpetrated only against large organizations. One report in a business magazine has estimated that 80 percent of all crimes involving businesses are associated with small businesses. Although the full impact of fraud within organizations is unknown, various national surveys have reported that annual fraud costs of U.S. organizations exceed $900 billion (or 7 percent of their revenues) and they are increasing (Weirich *et al.*, 2010). Fraud examinations and background checks are not easy tasks. One must have the proper training, skills, and experience to conduct a successful fraud investigation. Therefore, this study concentrates on these issues to fill this gap.

Also, the growth of information technology has been a positive force in business; but, as in the case with all innovations, it has a downside risk as well. Organizations, both large and small, have become to rely heavily on information technology to provide timely information used in making critical business decisions. As such, reliance on information technology grows, so do the risks which the organization faces. So, anyone involved in decision making should understand those risks and how they can impact the organization. Fraud is one of the business risks. A fraud is a dishonest act by an employee that results in personal benefit to the employee at the expense of the employer. Why does fraud occur? The three main factors that contribute to fraudulent activity are depicted by the fraud triangle: opportunity, financial pressure, and rationalization (For details, see Weygandt *et al.*, 2010). Fundamentally, computer fraud is people fraud; no computer system can perpetrate fraud without at least some human intervention[22]. The required computer skills will vary greatly depending on the type of fraud being perpetrated.

What can be done to prevent or to detect fraud? After numerous corporate scandals came to light in the early 2000s, The Congress addressed this issue by passing the Sarbanes- Oxley Act of 2002 (SOX). Under SOX, all publicly traded U.S. corporations are required to maintain an adequate system of internal control. Corporate executives and boards of directors must ensure that these controls are reliable and effective. In addition, independent outside auditors must attest to the adequacy of the internal control system. Companies that fail to comply are subject to fines, and company officers can be imprisoned. SOX also created the Public Company Accounting Oversight Board (PCAOB), to establish auditing standards and regulate auditor activity (for details, see Bawaneh, 2011b) and below is a brief description of a good internal control to help an organization achieve its objectives.

Internal Control

Internal Control consists of all the various methods and measures designed and implemented within an organization to achieve the following four objectives: (1) safeguard assets, (2) check the accuracy and reliability of accounting data, (3) promote operational efficiency, and (4) enforce prescribed managerial policies (Bagranoff *et al.*, 2010). An organization that achieves these four objectives is typically one with good corporate governance. This means managing an organization in a fair, transparent, and accountable

[21] More detailed discussion of the fraud can be found in the following: G. Jack Bologna and Robert J. Lindquist, *Fraud Auditing and Forensic Accounting* 2nd Ed. (New York: John Wiley & Sons, Inc., 1995); W. Steve Albrecht et al., *Fraud Examination* (Cincinnati: South-Western/ Cengage, 2009); and Association of Certified Fraud Examiners, *Fraud Examiners Manual*, annual editions.

[22] In 1989, the U.S. Department of Justice defined computer fraud as being any illegal act for which knowledge of computer technology is used to commit the offense.

manner to protect the interests of all the stakeholder groups[23]. Internal control systems have five primary components: a control environment, risk assessment, control activities, information and communication, and monitoring (Weygandt *et al.*, 2010). Each one of the five components of an internal control system is important, but the control activities are the backbone of the company's effort to address the risks it faces, such as fraud. The specific control activities used by a company will vary, depending on the management's assessment of the risks faced. This assessment is heavily influenced by the size and nature of the company. According to Weygandt *et al.* (2010), there are six principles of control activities which are applied to most companies and are relevant to both manual and computerized accounting systems: establishment of responsibility, segregation of duties, documentation procedures, physical control, independent internal verification, and human resource control.

Research Methodology

Undertaking research in the field of social sciences requires many ways to adopt, and this applies to accounting as a social practice. One of which is the case study, which is preferable for questions to "why" or "how", because the researcher has "no control over events" (Yin, 1984) and such questions deal with operational links which need to be traced over time, rather than by frequency (Bawaneh, 1997; 2011b) , and will focus on a contemporary phenomenon within a real-life context to be able to locate practice in its historical, as well as its economic and social contexts (Scapens, 1990).

This research conducts a case study method on security for bank within AIS to help determine the scope of computer crimes and fraud. The participants are the computer security practitioners and accountants in Jordan financial institutions. Thus, the case study approach helped this research to deal with multiple sources of evidence and to analyze the strengths and the weaknesses of processes reported by banks. The banks in Jordan were chosen on the basis of 'openness to society' access and the researcher had received full cooperation and support in his research from formerly university classmates, who were now top managers in the banking industry in Jordan.

This research utilized a variety of methods in collecting evidence to get close to the subject and to see the bank's social context from various perspectives, to gather more complete evidence on the issues under close examination, and to generate a rich source of field data by utilizing the "data-triangulation" approach to collect data. In doing this, many techniques were used covering interviews, participant observations, document analysis, archival records, and examination of newspaper reports (for review, see Bawaneh, 2011b).

Discussion of Findings and Analysis of Results

Based on previous information along with the theoretical argument presented in brief earlier, this study raises this specific question for analysis: what can organizations and accountants do to protect and secure their information resources from computer crimes, abuse, and fraud? This research paper aims at studying the dramatic changes that are occurring in the accounting environment such as: the new technologies which have an impact on many financial statement filings, new services that accountants are involved in and the need for specialized online database research skills which are continuously expanding.
n response to these changes in the accounting environment, accountants need to have the ability to cope with these changes and the need to use online databases as tools in gathering and organizing the evidence for the investigation of an accounting issue.

[23] "Corporate Governance: The New Strategic Imperative," A white Paper from the Economist Intelligence Unit, sponsored by KPMG International http://www.eiu.com.

What banks are doing to protect information resources? From the theoretical background mentioned earlier, Information resources are difficult to protect for many reasons: (1) IT security is the business of everyone in an organization (2) the online commerce industry is not particularly willing to install safeguards that would make completing transactions more difficult or complicated. Although, there are many major difficulties involved in protecting information, banks are developing software and services that deliver early warnings of trouble on the Internet. This early-warning systems are proactive, scanning the web for new viruses and alerting companies to the danger. Banks spend a great deal of time and money protecting their information resources. Before doing so, they perform risk management. A risk is the probability that a threat will impact an information resource. The goal of risk management is to identify, control, and minimize the impact of threats. In other words, risk management seeks to reduce risk to acceptable levels. Risk management consists of three processes: risk analysis, risk mitigation, and control evaluation. In control evaluation, the bank examines the costs of implementing adequate control measures against the value of those control measures. If the costs of implementing a control are greater than the value of the asset being protected, the control is not cost effective. To clarify this issue, the next section provides various control measures that banks use to protect their information resources.

To protect their information resources, banks implement controls, or defense mechanisms which designed to protect all of the components of an information system, including data, software, hardware, and networks. Controls are intended to prevent accidental hazards, deter intentional acts, detect problems as early as possible, enhance damage recovery, and correct problems.

In practice, banks adapted three types of control measures: physical controls which expected to prevent unauthorized individuals from gaining access to a company's facilities; access controls which expected to restrict unauthorized individuals from using information resources; and communications controls (also called *network controls*) which expected to secure the movement of data across networks. (For detail, see Rainer & Cegielski, 2013).

One key step in developing a secure network is to conduct a risk assessment. This assigns levels of risk to various threats to network security by comparing the nature of the threats to the controls designed to reduce them. It is done by developing a control spreadsheet and then rating the importance of each risk.[24] To be sure that the data communication network and microcomputer workstations have the necessary controls and that these controls offer adequate protection, it is best to build a control spreadsheet[25].

Ensuring business continuity: business continuity means that the organization's data and applications will continue to operate even in the face of disruption, destruction, or disaster. A business continuity plan has two major parts: the development of controls that will prevent these events from having a major impact on the organization, and a disaster recovery plan that will enable the organization to recover if a disaster occurs[26].

Intrusion prevention: intrusion is the second type of security problem and the one that tends to receive the most attention. No one wants an intruder breaking into their network. There are four types of intruders who

[24] CERT has developed a detailed risk assessment procedure called OCTAVE SM, which is available at www.cert.org/octave.

[25] Threats to the network are listed across the top, organized by business continuity (disruption, destruction, disaster) and intrusion, and the network assets down the side. The center of the spreadsheet incorporates all the controls that are currently are in the network. This will become the benchmark on which to base future security reviews (For details, see Dennis & durcikova, 2012, pp. 345-351.

[26] There are many good business continuity planning sites such as www.disasterrecoveryworld.com.

attempt to gain unauthorized access to computer networks. The first are casual intruders who have only a limited knowledge of computer security. The second type of intruders is experts in security, but their motivation is the thrill of the hunt. These intruders are called hackers and often have a strong philosophy against ownership of data and software. The third type of intruders, the most dangerous, is professional hackers who break into corporate or government computers for specific purpose, such as espionage, fraud, or intentional destruction. The forth type of intruder is also very dangerous. These are organization employees who have legitimate access to the network, but who gain access to information they are not authorized to use.

The key principle in preventing intrusion is to be proactive. This means routinely testing your security systems before an intruder does. Many steps can be taken to prevent intrusion and unauthorized access to organizational data and networks, but no network is completely safe. The best rule for high security is: do not keep extremely sensitive data online. Data that need special security are stored in computer isolated from other networks. In the same way that a disaster recovery plan is critical to controlling risks due to disruption, destruction, and disaster, a security policy is critical to controlling risk due to intrusion.

In the information age, fraud potential is wider in scope. However, new tools and techniques are available for accountants to combat this expansion of fraud. Uncovering signs of fraud among possibly millions of transactions within an organization requires the accountant to use analytical skills and work experience to construct a profile to test the data for the possibility of fraud. There are three important tools for the accountant, as a fraud examiner, such as data mining software, public databases, and the Internet.[27]

Conclusion and Recommendations

Before establishing the control procedures, banks recognized that, it is important to emphasize that the single most valuable control is user education and training. Therefore, most banks established center for training because they believe that an effective and ongoing education makes every member of the bank aware of the vital importance of information security.

Nonetheless, it is important to remember that it is not enough just to establish a series of controls; someone or some department must be accountable for the control and the security of the network. This includes being responsible for developing controls, monitoring their operation, and determining when they need to be updated or replaced. Controls reviewed periodically to be sure that they are still useful and must be verified and tested. Verifying ensures that the control is present, and testing determines whether the control is working as originally specified.

It is also important to recognize that there may be occasions in which a person must temporarily override a control, for instance when the network or one of its software or hardware subsystems is not operating properly. Such overrides should be tightly controlled, and there should be a formal procedure to document this occurrence should it happen.

[27] Following is a list of some of the more common commercial data mining software products used by fraud examiners: WizRule, Financial Crime Investigator, IDEA (Audimation Services, Inc.), Monarch, Analyst's Notebook (i2 Inc.), and ACL for Windows is the most commonly used software package. This software allows the fraud examiner to perform various analytical functions without modifying the original data. ACL is very beneficial in fraud detection due to its ability to quickly and thoroughly analyze a large quantity of data in order to highlight those transactions often associated with fraudulent activity.

Accountants are now being held professionally responsible for reducing risk, assuring compliance, eliminating fraud, and increasing the transparency of transactions according to generally accepted Accounting principles (GAAP). Furthermore, and in regards to the ethical issue, accountants now are being held professionally and personally responsible for increasing the transparency of transactions and assuring compliance with GAAP. The regulatory agencies, such as the SEC in the USA, require information security, fraud prevention and detection, and internal controls over financial reporting. Also, require accounting departments to adhere to strict ethical principles.

The accounting function is intimately concerned with keeping track of a bank's transactions and internal controls. Modern databases enable accountants to perform these functions more effectively. Databases help accountants manage the flood of data in today's organizations so that they can keep their firms in compliance with the standards imposed by e.g. Sarbanes-Oxley.

Good security for banks starts with a clear disaster recovery plan and a solid security policy which are not applied and many banks are not conducting a risk assessment procedure. Probably the best security investment in Jordanian banks is user training: training individual users on data recovery and ways to defeat social engineering. But this doesn't mean that technologies aren't needed either. Therefore, most banks now routinely use antivirus software, firewalls, VPNs, encryption, and IPS. So what may we expect in the future in "secure" organizational environments? This issue needs more research.

References

Aggarwal, R. and Samwick, A. 2006. Empire-Builders and Shirkers: Investment, Firm Performance, and Managerial Incentives, *Journal of Corporate Finance* 12, : 489-515.

Agrawal, A. and Chadha, S. 2006. Corporate Governance and Accounting Scandals, *Journal of Law and Economics* .48, : 371-406.

Albrecht, W. (2000). *Accounting Education: Charting the Course through a Perilous Future.* Sarasota, Fla.: American Accounting Association.

Albrecht, W., & and Sack, R. (2000). *Accounting Education: Charting the Course Through a Perilous Future.* Sarasota, Fla.: American Accounting Association.

Albrecht, W., Wernz, G., & and Williams, T. (1995). *Fraud: Bringing Light to the Dark Side of Business.* Burr Ridge, Ill.: Richard D. Irwin, Inc.

Anderson, K.L., Deli, D.N. and Gillan, S.L. 2005. Boards of Directors, Audit Committees, and the Information Content of Earnings, Working Paper, Arizona State University.

Arab Bank, Annual Report (2009).

Bagranoff, Nancy; Simkin, Mark; and Norman, Carolyn. (2010). *Core Concepts of Accounting Information Systems.* John Wiley & Sons, Inc.

Bawaneh, S. (1997, September). Management Performance in the Housing Bank in Jordan. *University of Manchester*, Manchester, UK: Unpublished PhD Thesis.

Bawaneh, S. (2011a). Information Technology, Accounting Information System and their Effects on the Quality of Accounting University Education. *Interdisciplinary Journal Of Contemporary Research In Business*, June Vol. 3, No. 2. forthcoming.

Bawaneh, S. (2011b). The Effects of Corporate Governance Requirements on Jordan Banking Sector. *International Journal of Business and Social Science* , May Special Issue Vol. 2 , No. 9, pp. 130-140.

Bhasin, M. L., (2013), Corporate Governance and Forensic Accountant: an Exploratory Study. *Journal of Accounting- Business & Management,* Vol. 20, No. 2, pp. 55-83.

Boone, A.L., Field, L.C., Karpoff, J.M. and Raheja, C.G. 2005. The Determinants of Corporate Board Size and Composition: An Empirical Analysis, Working Paper, Washington University.

Boostrom, R. (1992). *Developing Creative and Critical Thinking: An Integrated Approach.* Chicago: National Textbook Co.

Booth, J. and Deli, D.N. 1996. Factors Affecting the Number of Outside Directorships Held by CEOs. *Journal of Financial Economics* .40, : 81-104.

Brick, I.E., Palmon, O. and Wald, J. 2006. CEO Compensation, Director Compensation, and Firm Performance: Evidence of Cronyism? *Journal of Corporate Finance* 12, : 403-423.

Burrell, G. and Morgan, G. 1979. Sociological Paradigms and Organizational Analysis (London, U.K.: Heinemann).

Central Bank of Jordan, Bank Directors' Handbook of Corporate Governance (2004).

Central Bank of Jordan, Corporate Governance Code for Banks in Jordan (2007).

Chhaochharia, V. and Grinstein, Y. 2005a. The Transformation of US Corporate Boards: 1997-2003, Working Paper, Cornell University.

Chhaochharia, V. and Grinstein, Y. 2005b. Corporate Governance and Firm Value: The Impact of the 2002 Governance Rules, Working Paper, Cornell University.

Coles, J.L., Daniel, N. and Naveen, L. 2005 Boards: Does one Size Fit All? Working Paper, Arizona State University.

Dennis, A. and Durcikova, A. 2012, *Fundamentals of Business data Communications* 11th Edition (Singapore: Wiley & Sons).

Elliott, B. and Elliott, J. 2006. Financial Accounting, Reporting and Analysis: International Edition (Prentice-Hall).

Ferreira, L.D. and Merchant, K.A. 1992. Field Research in Management Accounting and Control: A Review and Evaluation, *Accounting Auditing & Accountability Journal* 5, (4) : 3-34.

Gillan, S.L. 2007. Recent Developments in Corporate Governance: An Overview 12: 381-402.

Gillan, S.L. and Starks, L.T. 1998. A Survey of Shareholder Activism: Motivation and Empirical Evidence, *Contemporary Finance Digest* 2: 10-34.

Gompers, P.A., Ishii, J.L. and Metrick, A. 2004. Incentives Versus Control: An Analysis of U.S. Dual Class Companies, Working Paper, Harvard University.

Guner, A.B., Malmendier, U. and Tate, G. 2005.The Impact of Board with Financial Expertise on Corporate Policies, Working Paper, Stanford University.

Hopper, T. and Powell, A. 1985. Making Sense of Research into the Organizational and Social Aspects of Management Accounting; A Review of its underlying Assumptions, *Journal of Management Studies* 22, (5) September: 429-465.

Hopper, T.M., Cooper, D.J., Lowe, T., Capps, T. and Mouritsen, J. 1986. Management Control and Worker Resistance in the NCB: Financial Control in the Labour Process, in Knights, D. and Willmot, H. (eds.), Managing the Labour Process (Aldershot: Gower).

Kelly Rainer, R. and Cegielski, C.G., 2013, *Introduction to Information Systems* 4th Edition (Singapore: Wiley & Sons).

Klock, M.S., Mansi, S.A. and Maxwell, W.F. 2005. Does Corporate Governance Matter to Bondholders? *Journal of financial and Quantitative Analysis* 40, (4): 639-719.

Lattemann, C., Fetscherin, M. Alon, I., Li, S. and Schneider, A. 2009. CSR Communications Intensity in Chinese and Indian Multinational Companies, *Corporate Governance: An International Review* 17, : 426-442).

Lee, T.A. 2006. Financial Reporting and Corporate Governance (Chichester: Wiley & Sons).

Lehn, K., Patro, S. and Zhao, M. 2005. Determinants of the Size and Structure of Corporate Boards: 1935-2000, Working Paper, University of Pittsburgh.

Lex, Big Government, Financial Times, March 21, 2005.

Linck, J.S., Netter, J. and Yang, T. 2005a. The Determinants of Board Structure, Working Paper, University of Georgia.

Linck, J.S., Netter, J. and Yang, T. 2005b. Effects and Unintended Consequences of the Sarbanes Oxley Act on Corporate Boards, Working Paper, University of Georgia.

Luck, D., Wales, H., & and Taylor, D. (1961). *Marketing Research.* Englewood Cliffs, N.J.: Prentice Hall Inc.

Morgan, G. and Smircich, L. 1980. The Case for Qualitative Research, *the Academy of Management Review* 5, (4): 491-500.

Morgan, G., 1983. Beyond Method: Strategies for Social Research (Beverley Hills, CA: Sage).

O'Regan, P. 2006. Financial Information Analysis (Chichester: Wiley & Sons).

OECD, Principles of Corporate Governance (1999). Available from World Wide Web:http//www.oecd.org/dataoecd/32/18/31557724.pdf

Otley, D.T. 1984. Management Accounting and Organization Theory: A Review of Their Interrelationships, in Scapens, R.W., Otley, D.T. and Lister, R. (eds.), Management Accounting, Organization Theory and Capital Budgeting: Three Surveys (London: Macmillan).

Paice, G. a. (2001, September). Addressing the People Puzzle. *Financial Executive*.

Resnick, L. (1987). *Education and Learning to Think.* Washington, D.C.: National Academy Press.

Roberts, D. 2004. A Shift in the Balance of Power, Financial Times, December 14.

Scapens, R. (1990). Researching Management Accounting Practice: The Role of Case Study Methods. *British Accounting Review* , 259-281.

Scapens, R.W. 1990. Researching Management Accounting Practice: The Role of Case Study Methods, *British Accounting Review* 22, : 259-281.

Shen, W. and Lin, C. 2009. Firm Profitability, State Ownership, and Top Management Turnover at the Listed Firms in China: A Behavioral Perspective, *Corporate Governance: An International Review* 17, : 443-456.

Shleifer, A. and Vishny, R. 1997. A Survey of Corporate Governance, *Journal of Finance* 52, : 737-775.

Sing, D.A., and Gaur, A. 2009. Business Group Affiliation, Firm Governance and Firm Performance: Evidence from China and India, *Corporate Governance: An International Review* 17, : 411-425.

Wallace, W. (Fall 1984). *A Profile of a Researcher, Auditor's Report.* American Accounting Association.

Weirich, T., Thomas, P., & and Churyk, N. (2010). *Accounting & Auditing Research Tools and Strategies.* John Wiley & Sons, Inc.

Weygandt, J., Kimmel, P., & and Kieso, D. (2010). *Accounting Principles.* John Wiley & Sons, Inc.

Yin, R. (1984). *Case Study Research: Design and Methods.* Beverly Hills, CA.: Sage.

Zattoni, A., Pedersen, T., and Kumar, V. 2009. The performance of Business Group Firms during Institutional transition: A Longitudinal study of Indian Firms, *Corporate Governance: An International Review* 1, :510-523.