2018

The relevance of a good internal control system in a computerised accounting information system

Raymond Lutui

Tau'aho 'Ahokovi

DOI: 10.25958/5c5270a16668d

Lutui, R., & 'Ahokovi, T. (2018). The relevance of a good internal control system in a computerised accounting information system. In *proceedings of the 16th Australian Information Security Management Conference* (pp. 29-40). Perth, Australia: Edith Cowan University.

THE RELEVANCE OF A GOOD INTERNAL CONTROL SYSTEM IN A COMPUTERISED ACCOUNTING INFORMATION SYSTEM

Raymond Lutui[1], Tau'aho 'Ahokovi[2]
Auckland University of Technology[1], Christ's University in Pacific[2]
rlutui@aut.ac.nz[1], tahokovi@bigpond.com[2]

Abstract

Advancements in information technology (IT) have enabled companies to use computers to carry out their activities that were previously performed manually. Accounting systems that were previously performed manually can now be performed with the help of computers. With all the advantages of computerized accounting software, business owners need to realize that problems do arise for a variety of reasons. Dependence on computers sometimes leads to bigger problems. This paper, therefore provide a detail information about the concept of internal control to its relevance in a computerised accounting information. This study also considers the trend between manual and computerised accounting system. This study concludes with recommendations on how to maximise the effectiveness of developing internal control systems of the computerized accounting systems which are characterized of providing appropriate safety to the systems. The systems can provide information characterized by reliability for the sake of taking decisions. These systems should integrated with other administrative and organizational systems.

Keywords

Accounting Information System, Internal Control System, Computerised Accounting System

INTRODUCTION

The world is changing faster than ever before as computer is affecting every sectors of the economy. Accounting profession is not left out of this change as the quality of information to be provided to users for decision making have to be improved on. The ongoing revolution in information technology (IT) has had a significant influence on accounting information system (AIS). Improvements in the IT have brought improvements in computers. Today, almost all organizations are using computers in their daily businesses. As computers become smaller, faster, easier to use, and less expensive, the computerization of accounting work will continue. Accounting activities that were previously performed manually can now be performed with the use of computers. That is, accountants are now able to perform their activities more effectively and efficiently than before. An accounting information system can be a manual system, or a computerized system using computers. Regardless of the type, AIS is designed to collect, enter, process, store, and report data and information.

According to Weber (2011), "Computerized accounting system (CAS) involves the use of computers in processing accounting data into information to facilitate quick decision making through timely preparation of financial reports and financial reporting in this case refers to the way in which financial information is recorded, processed and conveyed to the end users of this information in particular".

Accounting systems contain confidential information that should be kept safe and secure at all times. The consequences of unauthorized access can be devastating--from identity theft problems to loss of irreplaceable data. When accounting data is changed or deleted on purpose or by chance, it creates havoc in the accounting department, calling into question the reliability or accuracy of all data.

The internal controls of an AIS are the security measures it contains to protect sensitive data. These can be as simple as passwords or as complex as biometric identification. An AIS must have internal controls to protect against unauthorized computer access and to limit access to authorized users which includes some users inside the company. It must also prevent unauthorized file access by individuals who are allowed to access only select parts of the system. An AIS also needs internal controls that protect it from computer viruses, hackers and other internal and external threats to network security. It must also be protected from natural disasters and power surges that can cause data loss

LITERATURE REVIEW

The internal controls of an AIS are the security measures it contains to protect sensitive data. These can be as simple as passwords or as complex as biometric identification. An AIS must have internal controls to protect against unauthorized computer access and to limit access to authorized users which includes some users inside the company. It must also prevent unauthorized file access by individuals who are allowed to access only select parts of the system (Romney, Steinbart & Cushing, 2000).

Quality, reliability and security are key components of effective AIS software. Managers rely on the information it outputs to make decisions for the company, and they need high-quality information to make sound decisions. AIS software programs can be customized to meet the unique needs of different types of businesses. If an existing program does not meet a company's needs, software can also be developed in-house with substantial input from end users or can be developed by a third-party company specifically for the organization. The system could even be outsourced to a specialized company (Pahnila, Siponen & Mahmood, 2007).

Ge and McVay (2005) claim that, for publicly-traded companies, no matter what software program and customization options the business chooses, Sarbanes-Oxley regulations will dictate the structure of the AIS to some extent. This is because SOX regulations establish internal controls and auditing procedures that public companies must comply with.

An AIS also needs internal controls that protect it from computer viruses, hackers and other internal and external threats to network security. It must also be protected from natural disasters and power surges that can cause data loss. We've seen how a well-designed AIS allows a business to run smoothly on a day-to-day basis or hinders its operation if the system is poorly designed. A third use for an AIS is that when a business is in trouble, the data in its AIS can be used to uncover the story of what went wrong (Simkin, 2006).

The control environment is the overall attitude and tone of an organization toward internal control. Often talked about as "tone at the top," an effective control environment starts with management that is interested in such controls. The control environment affects a company's internal control through explicit and implicit actions. Explicitly, a strong control environment is shown through management taking time to design and implement internal controls, monitor risk and communicate the results to employees. Implicitly, strong control environments are demonstrated by management that doesn't tolerate circumnavigation of controls and clamps down on those who bypass the control system (Rae & Subramaniam, 2008).

Risk assessment means determining how relevant risks affect the business objectives of your company. An effective internal control system has internal controls mapped to the risks that could impede the company's success. Of course, mapping controls to risk requires that you identify these risks in the first place. This is where the risk assessment component of the framework comes in. A best practice is to perform an annual risk assessment during the company budget process (Collier, Berry & Burke, 2006).

A business can design the best internal control system in the world, but if employees don't know about it, there is little chance of it benefiting the company. The information and communication part of the internal control framework is charged with making sure that information gets where it needs to be in the organization. While this includes information from company management getting to employees, it also includes information from employees making it to management. For example, implementation of a policy to report suspected fraud would be included in the information and communication part of the framework.

The monitoring part of the internal control framework is somewhat like an annual check-up for the control system. Even the best internal control systems should adapt to changes in the company or the business environment. To check for these changes, small businesses should conduct periodic evaluations of the entire internal control system and act on the results of these evaluations (Spira & Page, 2003).

When most people think about internal control, control activities are what come to mind. These are the specific actions that management and employees take to maintain internal control. For example, a company determines during the risk assessment that theft of cash is a risk to the company's profitability. The company then designs a control to counter the risk. For this example, the company may implement that only one person uses a cash drawer on a shift. The rule of one person per cash drawer is the control activity in this situation.

The concept of accounting information systems (AIS) and their components is a system that collect, record, store, and process the data to provide the information for decision-making. (Eppler & Mengis, 2004).

It can be defined as well as a set of processes of input, processing and output. It must be characterized by the information resulting from the accounting system of a range of characteristics, including the following:

1) Relevant: if the information is appropriate, reduced uncertainty, and improved the ability of decision makers to predict alleged, confirmed, or corrected their expectations for the future.
2) Reliability: the information considers reliability if they are correct, non-biased and expresses accurately for events or activities of the company.
3) Complete: if not deleted an important aspect from the events or from activities that the information measures them, then this information be complete.
4) Understandable: information become understandable when provide it in understanding and useful form.
5) Verifiable: the information is verifiable when we reach to the same information by two independent persons.

Components of Accounting Information Systems (AIS):

1) System operators and who do the different tasks.
2) Data relating to the facility and its operations.
3) The software used for data processing facility.
4) Infrastructure for information technology, which includes computers, peripherals, networks used for the collection, storage, processing and transmission of data and information.

CONTROL ACTIVITIES, BUSINESS PROCESSES AND ACCOUNTING

In conceptualizing accounting, business processes and internal controls, it is useful to think of the financial reporting process and the possibility of errors occurring in that process. While the scope of internal controls extends beyond the domain of the financial reporting process, commencing from the accounting process and branching out will allow you to start a foundation that will seem familiar to your understanding (Bodnar & Hopwood, 2001).

Once an organization has identified a source of risk its next step is to evaluate the extent of the risk. For example, let's assume the simple example of a sales process requiring that a sales order form be filled in, with this form stored until the end of the day. At the end of the day, the form is entered into the computer and the sales and accounts receivable balances are updated. If we now think about the risks involved in this process, or what could go wrong, perhaps surprisingly, given the somewhat simple nature of the process, there are several areas for potential errors (Romney, Steinbart & Cushing, 2000). These include:

1) incorrect details being recorded on the sale order form
2) the sale order form being lost/damaged
3) the sales order form data being entered incorrectly
4) accounts receivable and sales data being updated incorrectly
5) the computer system not being available
6) unauthorized people accessing the computer and entering transactions, either incorrectly, due to lack of knowledge of the process, or falsely, for motives of fraud or personal gain.

From the small business process example, we can ask what could go wrong and come up with six potential threats to the recording and processing of the sales order form. Let us think about how these errors relate to the financial statement assertions. Let's assume that two sale order form have been filled in incorrectly but one has been lost and the other was entered incorrectly into the computer. This means that there is one sale that will not be recorded. As a result, we immediately have a concern about the sales figure that will be contained in the financial statements since it will not include all sales made. We would also have a concern about the valuation of accounts receivable and inventory, since accounts receivable would be understated and inventory would be overstated. With the incorrectly entered form, let's assume that the quantity sold was keyed in as 78 instead of 67 units. As a result of this error, the sales figure will be higher than it should be, accounts receivable will be higher than it should be and inventory will be lower than it should be.

From these two examples, we can see how an error in a business process can impact the financial statements (Poston & Grabski, 2001). However, it is not only financial statement errors that internal controls are concerned with. As accountants and auditors will likely primarily be exposed to the financial statement perspective, but it should also be aware of the environment in which the financial statements are generated and think also in terms of the risks that do not directly impact on the financial statements. After identifying risks, management will decide on an appropriate policies and procedures to address risks. These policies and procedures are called control activities, and will be communicated to the organization for implementation.

TYPES OF CONTROL ACTIVITIES

From the COSO (Committee of Sponsoring Organisation) framework, one of the components of the internal control system was control activities. As a starting point, we look at the classification provided by Australian Auditing Standards (McNally, 2013). Financial statement auditors use the auditing standards as a basis for planning and carrying out external financial statement audits with the aim of detecting and material misstatements in the financial statements. The auditor's concern, therefore, is primarily with the financial accuracy of the statements. However, note that, while the auditing perspectives provides us with a basis for our controls, for an accountant working with an accounting information system within an organization, the concern extends beyond financial to non-financial risks and controls. Australian Auditing Standard ASA 315 identifying and assessing the risks of material misstatement through understanding the entity and its environment classifies controls into five types:

1) authorization
2) performance review
3) information processing controls
4) physical controls
5) segregation of duties

This perspective on control activities focuses on the risk areas/activities within the organizations and emphasizes a functionalist perspective in what happens within the organization and how the controls operate. These control areas should be emphasized, which each would show different examples of specific control activities (Rahman, 2013). Authorization is concerned with the activities, procedures put in place to reasonably assure that the transactions, those with the appropriate authority carry out events occurring, and that such events have been appropriately approved prior to execution. Performance reviews are those activities that involve some form of review or analysis of performance, typically looking to compare actual outcomes with those that were expected or planned.

Information processing controls are those that are put in place within the organization to work towards the accuracy, completeness and authorization of transactions. Accuracy is the aim of making sure that all data that enters the system are correct and reflect the actual events that are being recorded. Completeness refers to the aim of ensuring that all events that occur are recorded within the system. Information processing controls can be classified as either general or application controls.

General controls are those policies and procedures that relate to many applications and support of effective functioning of application controls by helping to ensure the continued proper operation of information systems. Application controls apply the processing of individual applications or processes. These controls help to provide reasonable assurance that all transactions have occurred, are authorized, and are completely and accurately recorded and processed. As the name suggests, physical controls refer to those controls that are put in place to physically protect the resources of the organization, including to protect them from the risk of theft and damage.

Segregation of duties refer to the concept that the same person should not perform certain key functions. The typical reference point within a business process is whether the record keeping the person who records a transaction, execution a person who performs a transaction, custody is a person in possession of the assets involved in a transaction and reconciliation is a person reconciling transaction data that should be separated. These alternatives classification of controls is by no means in conflict. Rather, they represent the numerous perspectives that can be taken when analysing internal controls. Controls may also be classified based on how they deal with risk and where in the information processing activities they operate (Bonabeau, 2002). These include classifications of preventive/ detective/corrective controls and input/processing/ output controls.

PREVENTIVE, DETECTIVE AND CORRECTIVE CONTROLS

Control activities can be broadly classified as preventive, detective or corrective. This classification views control activities based on how they deal with the risks that confront the organization, do they stop the risk from materializing, detect when a risk has materialized or remedy the situation after the risk has come to fruition. This obvious preference is for preventive controls which those that stop all risks from occurring. However, this is not always possible, which in some risks it will not be anticipated and, as a result, no preventive strategies will have been put in place. It may not be possible to prevent or detect some risks leaving corrective controls as the only option (Kliem, 2004). For some risks, even if we anticipate their occurrence, we may not put in place control activities to address them.

Preventive controls are designed to stop errors or irregularities occurring. Detective controls will not prevent errors from occurring. Rather the function of a detective control is to alert those involved in the system when an error or anomaly occurs. An example is the use of a virus scan program to check for computer viruses.

Corrective controls are designed to correct an error or irregularity after it has occurred. Examples include the organization's disaster recovery plan, which aims to restore the business to an operating position after the occurrence of a disaster, and the use of virus protection software to remove a virus that has corrupted computer programs within the organization. However, if the virus definitions on a scan program are not up to date, a virus will not be known until it has caused damage to data or network operation. Corrective control comes into effect after error or irregularity has occurred. This classification scheme of preventive and corrective controls can be applied to both general and application controls.

COSO, COBIT AND CONTROL ACTIVITIES

The COSO framework for internal control provides a framework that has received endorsement from US authorities, with the Securities and Exchange Commission, which requires the use if an internal control framework that has been extensively developed and publicly distributed (Moeller, 2013). COBIT (Control Objectives for Information and Related Technologies) 4.0 and follow up version COBIT 4.1 are widely applied frameworks for internal control that are often used by organizations as an addition to the COSO framework and a source of IT specific control objectives. Released by the IT governance institute, they provide a structure within which an organization can assess its controls and identify the need for controls at the various stages of the IT lifecycle.

Table 1: Control issues at various data processing stages

	Aim	**Control Issues**	**Example of controls**
TRANSACTION AUTHORISATION	Document preparation	Is data gathered accurately?	Pre-formatted documents. Review of documents.
	Authorization to prepare documents	Was the preparer authorized to prepare the document? Are prepared documents reviewed?	Job descriptions defining responsibility. Segregation of preparation and approval responsibilities. Review of prepared documents. Restricted access to blank source documents.
	Documentation collection	Are source documents complete? Accurate? Are all source documents accounted for? Are source documents moved through the process in a timely manner for input into the system?	Pre-numbered documents. Sequence checks. Batch totals. Cancelling source documents after completion of transaction.
	Document storage	Are documents kept to allow preservation of an audit trail? Are documents kept for required legal time frame?	Maintenance of secure storage systems

DATA INPUT	Authorized entry	Is the person entering the data authorized to?	Job description defining responsibility. System access controls. Login procedures. Defined user privileges. Time-out after inactivity. Separation of duties. Data entry and data file maintenance or update.
	Checking for accuracy, completeness and authorization	Does the system check for accuracy? Does the system check for completeness? Does the system check for validity? When is the data gathered and entered?	Edit checks. Reasonableness. Range checks. Limit checks. Logic checks on entered data. Redundant data check. Completeness checks. Require fields. Batch totals. Reconciliation of transactions entered and transactions processed.
			Capture data at its point of origin. Turnaround documents. Use of a standard chart of accounts.
DATA PROCESSING	Integrity	Is processed data verified as being correct? Are checks in place to ensure data updates have occurred correctly?	Run to run totals. Batch totals. Comparison of source documents to updated data files. Sequence checks. Processing error logs
DATA OUTPUT	Storage	How long is output stored for? Where is output stored? What privacy and security issues impact on the treatment of outputs?	Defined policies for the storage of outputs. Defined policies for the distribution of documents.
	Access	Who can access the outputs?	Printing to secure locations for sensitive material. Defined user privileges for accessing or printing outputs. Defined job descriptions or role responsibilities that specify required outputs.

	Checking	Are the outputs accurate? Is an adequate audit trial maintained? Are procedures in place for any detected errors?	Reconciliation of outputs to source data Reconciliation of subsidiary and control accounts
EXTERNAL DATA	Reliability	Is the data accurate? Is the data valid? Is the data complete?	Confirmation of details with third parties. Within firm authorization, (e.g. credit checks for sales orders received by fax). Checking that the third party (supplier or customer or creditor) is unknown to us. Use of existing customer or supplier, or credit data to confirm existence. Use of turnaround documents.

AIMS OF A COMPUTERISED ACCOUNTING INFORMATION SYSTEM

Any computerized system should aim to ensure transactions are properly, authorized, recorded and processed in their entirety in a timely manner (Apap et al., 2011).

Proper Authorization

The aim of proper authorization is to ensure that those people with the appropriate authority execute transactions, and that the appropriate people perform any modifications to the data in the system. That is, the transaction must be authorized. Authorization in a computerized information system can be established through user privileges and access rights by placing restrictions on what different users are able to do within the system.

Proper Recording

Proper recording of transactions is essentially about accuracy. Accuracy is concerned with making sure that all data enter the system are in the correct format and of the right type, and that the data gathered accurately reflect the reality of the underlying transaction or event. As an example, if the data field for the staff numbers on a data base is preformatted to contain only six numerals then it should not be possible to enter a staff number that contains alphabetic characters or numbers with five or seven digits. It would also be required that staff numbers entered are valid, that an employee within the organization actually has the staff number.

Completeness

Completeness can refer to both inputs to the system and transactions handled by the system. Input completeness is the aim of ensuring all transaction events and all required data relating to those events are captured within the system.

Timeliness

The goal of timeliness works towards ensuring that data are captured, processed, stored and made accessible. This is to enable the production of useful information for system users. Timeliness for an information system does not necessarily mean that all transactions must be processed immediately, rather that they should be processed to suit the need to the organization.

GENERAL CONTROLS

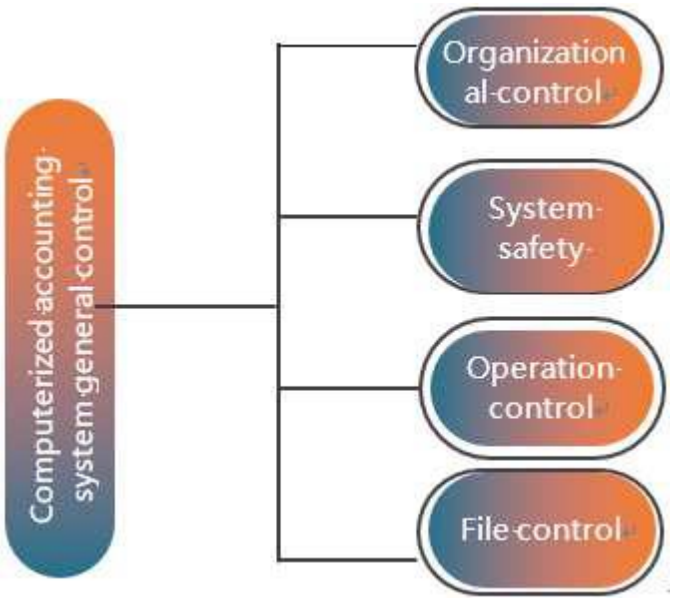

Figure 1. General control content of computerized accounting system

General controls are those that relate across all the information systems in an organization. They include the areas of physical controls, segregation of duties, user access, systems development procedures, user awareness of risks and data storage procedures (Ouchi, 1979).

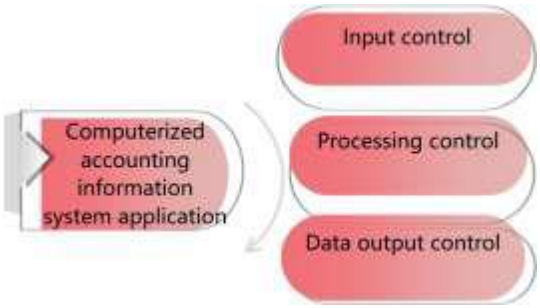

Figure 2. Computerized accounting information system application control category

Physical Controls

Physical controls are concerned with restricting access to the physical resources of the organization's computing resources. Especially for organizations that have large data processing centres that handle all of the transactions and information processing requirements of the organization, the risk of unauthorized people accessing and damaging the physical infrastructure is one of the organizations will not be prepared to take. As a result, organisations will employ a range of physical controls to restrict physical access, including:

- Locked computing premises- Locking facilities and restricting the distribution of keys to the facility works in two ways. First, the locked premises mean that unless you have a key you are unable to gain access. Second, if the distribution of keys is controlled it is possible to narrow down the people who may have entered the premises at a particular time. Locking premises is primarily a preventive control; it stops unauthorized access to the premises.
- Discrete premises that do not attract attention- Discrete premises can be a consideration when choosing the location for data processing and technology headquarters. Organizations that not advertise the location of their information technology centres are theoretically less exposed to targeted attacks on the organization's physical resources.

- Swipe card access- Controlling physical entry to buildings and office facilities through the use of swipe card access means only those with a swipe card will be able to gain access. Swipe card technology also allows for the recording of data about who enter the premises and what time.
- Biometric access controls- A limitation of swipe cards is that the person with the card may not necessarily be the person who is meant to have the card, since swipe cards may be lost, stolen or loaned. A way to overcome this is through the use of biometric controls, such as finger print swipes or retina scans. The benefit of this technology is that biometric identification, unlike swipe cards or passwords, ensures that the person gaining access is actually authorized to do so.
- Onsite security- The presence of onsite security, such as a manned front desk, can be an effective means of restricting unauthorized people from accessing a building.
- Security cameras to record access to the premises- the presence of security cameras can act as both a preventive and a detective access control. From preventive perspective, if people know cameras are there they are less likely to attempt unauthorized access. Additionally, if the cameras are present they can provide a means of detecting unauthorized access.

Segregation of Duties

The recording, execution, custody, authorization and reconciliation functions should be performed by different individuals. When looking at IT systems, separation of duties is equally important. Within the IT function, separation of duties should exist between the users of IT, the maintainers of the IT systems, system designers, system testers and those with access to the data within the systems. The rationale behind this is that combining any of these roles creates a conflict for the individual, places the organization's resources at risk and enables an individual to carry out fraud without being detected. For example, if the person designing and testing a new application also has access to the organization's data resources there is the possibility that the live data could be used in the testing process.

User Access

The area of user controls predominantly relates to the logical access of users to the systems within the organization. The primary example in this area is the use of passwords to restrict system access to authorized users by allocating users a unique identification code that only they are aware of, as well as on of the most common access control methods in operations. Organizations requiring users to have passwords need to consider the following aspects of password operation.

What Format is the Password?

Increased sophistication in the development of algorithms and programs designed to break passwords means that password strength becomes and important issue. The strength of the password is related to its length and format. For example, a password that is set as 'CAT' would be much easier to crack than a password that has been as 'C@9at12#'. Increasingly, online sites that require passwords will provide indicators of password strength, with many advocating mixes of alphanumeric characters, upper- and lower-case characters and symbols (Zhang, Monrose & Reiter, 2010).

What is the Life of the Password?

Increased security comes from passwords that are required to be changed on a regular basis, since the more the password is changed the more the risk of them becoming known is reduced. As a result, some systems will require users to change their password on a regular basis like every four weeks.

Is the Password Unique?

A user may have access to several different systems or modules within a system. If each of these requires a password, the potential exists for the user to have numerous passwords. Again, this may lead to confusion for the user in trying to remember their various access codes. The temptation for users may be to use the same password for various system. For example, you may use the same password for your email, eBay, amazon and YouTube accounts. Research found that typical internet user may have access to as many as 5 different accounts, each requiring a user identification and password.

What happens if a Login is Unsuccessful?

If a user forgets their password they will not be able to access their account. A system should be configured to log unsuccessful login attempts. Keeping a log of unsuccessful login attempts can be useful for following up on potential attacks. Analysis may reveal that attempts happen at a particular time or through a particular user name. This could prompt further investigation. In addition, some systems may freeze an account after a number of consecutive failed login attempts. Typically, after three unsuccessful login attempts, an account may be frozen. This control works to stop systematic attempts at determining a user's password. Once an account is frozen the fact should be logged and the user required to apply a password reset.

Security of the Password

Given the most system users will have multiple passwords, the tendency is for these to be written down. From a control perspective, the writing down of passwords should raise questions about where the documents containing the passwords is then stored. For example, storing the passwords in a notebook that is locked in a desk drawer or filing cabinet if preferable to recording them on a post it notes affixed to the computer screen where anyone can access them. A survey conducted by charted accounting firm Ernst & Young reported that the most common IT internal control issue faced by organizations related to security and user access. See figure 3. This would encompass the issues of user verification and password design and implementation. Issues to be considered and addressed include the format of the password, the process for creating and removing user accounts and user training about issues of security and password policy. Other issues that are commonly present include those related to the protection of the IT infrastructure, data protection, and change controls relating to how IT change is managed and carried out within the organization (Ashbaugh-Skaife, Collins & Kinney Jr, 2007). The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. Journal of Accounting and Economics, 44(1-2), 166-192.)

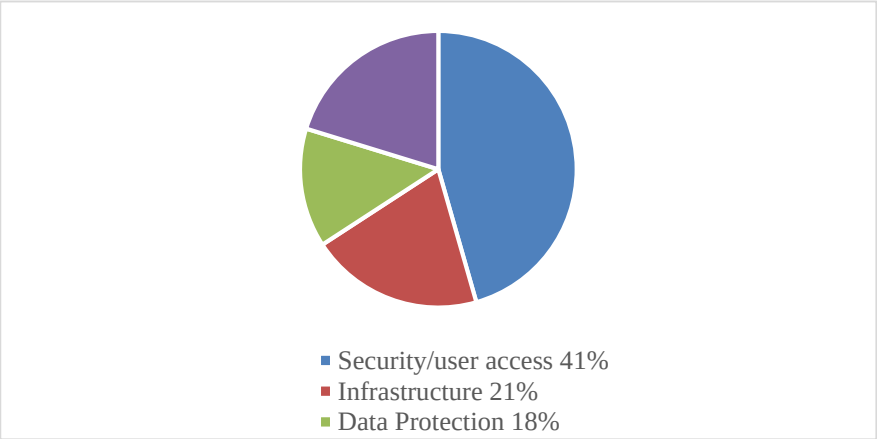

Figure 3: IT control issues faced by organisation (Ernst & Young 2005)

Security controls

Security controls refers to tools that provide security services, for example passwords and firewalls. Information systems security control is a means of ensuring business continuity and minimizing business damage by preventing and mitigating the effect of threats to the system (Dhillon, 1995; von Solms, 1998).

TRENDS BETWEEN MANUAL ACCOUNTING AND COMPUTERIZED ACCOUNTING SYSTEMS

While manual accounting system is tedious and time consuming, it offers some benefits. The ledgers are easy to review, and Accountants can make simple changes if necessary; individual accounts are easily reconciled because information is in a systematic order through each ledger. Accountants also have the benefit of physically handling each ledger and creating notes in customer accounts regarding any issues that need clarification or corrections. However, computerized accounting offers several more benefits than manual accounting; accountants process more information quicker, formulas verify calculated totals, therefore errors are less common. Accounting systems

also are customizable by industry, allowing accountants the opportunity to use preset templates for their general ledger. Accountants also can store several years of financial information with relative ease, giving them the opportunity to review previous year's information without sorting through stacks of paper ledgers. Most companies will use a computerized accounting system for recording and presenting their financial information. This system allows companies to record business transactions accurately and generate financial reports quickly for management review (Mohammed, 2004). While the functions of manual accounting have changed, it will never go away completely. Accountants must review the information presented on financial reports from the accounting system and ensure that it is accurate and valid. Accountants must also ensure that all financial information follows the Generally Accepted Accounting Principles and any other guidelines from regulatory agencies (Beirstaker, Bumaby & Thibodeau, 2001).

RECOMMENDATION

Based on the findings of this research, the following recommendations were made:

1) The necessity to increase the interest in developing effective internal control systems of the computerized accounting systems which are characterized of providing appropriate safety to the systems so as the systems can provide information characterized by reliability for the sake of taking decisions and these systems should integrated with other administrative and organizational systems in the organisation.
2) The necessity of the keeping up with the continuous technological development and getting benefit of all the areas of development regarding the maintenance of the security and safety of the information as possible.
3) The organisation should hold continuous training courses to the old and new employees to show them the importance of their commitment to the control procedures regarding the safety and security of the computerized accounting systems and train them to use procedures.
4) The organisation's adoption of a special system regarding the preventive procedures of the risks of the computerized accounting systems.
5) Each jurisdiction legislative power should increase the penalties regarding the electronic crimes especially what is concerning the penetration of the organisation systems and playing with for what this penetration caused as great harm on the shareholders of the organisation.
6) The organisations should use the international accounting standards as accepted by the government and international financial reporting standards.

CONCLUSION

At the organizational level, internal control objectives relate to the reliability of financial reporting, timely feedback on the achievement of operational or strategic goals, and compliance with laws and regulations. Internal control plays an important role in the prevention and detection of fraud. Under the Sarbanes-Oxley Act, companies are required to perform a fraud risk assessment and assess related controls. This typically involves identifying scenarios in which theft or loss could occur and determining if existing control procedures effectively manage the risk to an acceptable level. The risk that senior management might override important financial controls to manipulate financial reporting is also a key area of focus in fraud risk assessment. Controls can be evaluated and improved to make a business operation run more effectively and efficiently. For example, automating controls that are manual in nature can save costs and improve transaction processing. If the internal control system is thought of by executives as only a means of preventing fraud and complying with laws and regulations, an important opportunity may be missed. Internal controls can also be used to systematically improve businesses, particularly about effectiveness and efficiency.

REFERENCES

Amy Fontinelle | Updated February 21, 2018 — 10:30 AM EST Introduction to Accounting Information Systems

Apap, F., Honig, A., Shlomo, H., Eskin, E., & Stolfo, S. J. (2011). U.S. Patent No. 7,913,306. Washington, DC: U.S. Patent and Trademark Office.

Ashbaugh-Skaife, H., Collins, D. W., & Kinney Jr, W. R. (2007). The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. *Journal of Accounting and Economics*, 44(1-2), 166-192.

Beirstaker, J.L. Bumaby, P., Thibodeau, J. (2001), the impact of information technology on the audit process:

Bodnar, G. H., & Hopwood, W. S. (2001). *Accounting information Systems.*

Bonabeau, E. (2002). Agent-based modeling: Methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences*, *99* (suppl 3), 7280-7287.
Collier, P. M., Berry, A. J., & Burke, G. T. (2006). Risk and management accounting: best practice guidelines for enterprise-wide internal control procedures (Vol. 2, No. 11). Elsevier.
Eppler, M. J., & Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. The information society, 20(5), 325-344.
Dhillon, G. (1995) Interpreting the Management of Information Systems Security, London: London School of Economics and Political Science.
Ge, W., & McVay, S. (2005). The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizons*, *19*(3), 137-158.
Hanini, E.: 'The Risks of Using Computerized Accounting Information Systems in the Jordanian banks; their reasons and ways of prevention', *European Journal of Business and Management*, 2012, 4, (20), pp. 53-63
Kliem, R. (2004). Managing the risks of offshore IT development projects. *Information Systems Management*, *21*(3), 22-27.
McNally, J. S. (2013). The 2013 COSO Framework & SOX Compliance: One approach to an effective transition. *Strategic Finance*, 45-52.
Moeller, R. R. (2013). *Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework*. John Wiley & Sons.
Mohammed S.R. (2004), financial statement analysis - auditing practice: S Olajide and company Ibadan, Oyo
Osmond V, (2011): Manual versus Computerized Accounting Systems. Introduction To Accounting Information Systems
Ouchi, W. G. (1979). A conceptual framework for the design of organizational control mechanisms. In *Readings in accounting for management control* (pp. 63-82). Springer, Boston, MA.
Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on* (pp. 156b-156b). IEEE.
Poston, R., & Grabski, S. (2001). Financial impacts of enterprise resource planning implementations. *International Journal of Accounting Information Systems*, *2*(4), 271-294.
Rae, K., & Subramaniam, N. (2008). Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud. *Managerial Auditing Journal*, *23*(2), 104-124.
Rahman, A. R. (2013). *The Australian Accounting Standards Review Board (RLE Accounting): The Establishment of its Participative Review Process*. Routledge.
Romney, M. B., Steinbart, P. J., & Cushing, B. E. (2000). *Accounting information systems* (Vol. 2). Upper Saddle River, NJ: Prentice Hall.
Schneider, A.: 'The reliance of external auditors on the internal audit function', *Journal of Accounting Research*, 1985, pp. 911-919
Schneider, A.: 'The reliance of external auditors on the internal audit function', *Journal of Accounting Research*, 1985, pp. 911-919
Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640-661.
Von Solms, R. (1998) "Information security management: the code of practice for information security management", Information Management and Computer Security, vol. 6(5): 224-225
Zhang, Y., Monrose, F., & Reiter, M. K. (2010, October). The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 176-186). ACM.