Research Journal of Finance and Accounting
ISSN 2222-1697 (Paper) ISSN 2222-2847 (Online)
Vol.4, No.1, 2013

Evaluating internal controls in a computerised works environment – a risk to audit professionals and a challenge to accountancy training providers

Sampson Anomah,
Lecturer, (in Accounting Information Systems),
Department of Accountancy
Kumasi Polytechnic,
P.O Box KS 7811, Adum, Kumasi – Ghana
Email: samanomah@msn.com
Phone: 00233-245-225-483

Owusu Agyabeng
Lecturer, Department of Accountancy
Kumasi Polytechnic,
Email: oadjass@yahoo.com

Abstract:
Information and Computer technology (ICT) has become integral part to any modern accounting information systems. ICT, however, is a high risk discipline due to high level of vulnerabilities and threats. A key emphasis ofauditing procedures is identifying risks, fraud and errors by making inquiries of and testing Internal controls within the entity in order to place some reliance on internal reports and associated management assertions. Auditors' responsibility in identifying fraud has now been acknowledged by regulatory standards and the law. It has become critical that auditors are fully aware of the impact of ICT issues on the audit of a client's financial statements in howICT is used by a client to gather process and report financial information.It is, therefore, recommended that accountancy training institutions kept pace with time and inculcated into their training more skills in ICT relevant to their field to improve on the quality of professionals. This article makes use of extensive review of literature with some empirical knowledge to aid the analysis of the available literature.
Keywords: Auditors, internal control, challenges, accounting, information technology, risks, skills, training.

1.0. Introduction

The accountancy profession now faces a challenge to recover trust and respect. The reputation of the profession has been damaged by high-profile scandals such as Enron, WorldCom and Parmalat. Those scandals have created some suspicion of accountants among the public on the competence of auditors and the accountancy profession as a whole. Internal controls have been a very important topic in recent years. Many people have postulated that one major critical success factor of any competitive business is its effective internal controls. The world is now a global village as predicted due to the Information and Computer technology (ICT). Sophisticated ICT has become integral part in modern accounting information systems and management information systems. This has affected the traditional procedures auditors employ to perform their procedures. Normally, though, they only possess ordinary skills to work with Computers. Their competence and professionalism to take up engagements in the face of the sophistication in ICT use that is fast complicating the internal control environments are called to question. Auditing procedures in identifying risks, fraud and errors by making inquiries of and testing internal controls within the entity have changed as a result and therefore the competence and skills of the auditor must change to suit the circumstance to minimise audit risks that would add to the worsened reputation of the profession.

1.1. Background study:

As a result of some notorious recent audit failures involving large corporations around the world especially in the United States, the Sarbanes Oxley Act (SOX) was enacted in United States of America since 2002. This ACT has become a de facto international standard for good governance and controls of Companies. It requires that (Section 302) the chief executive and chief financial officers of public companies attest to the accuracy of financial reports

and auditing process, in most cases, must provide a reasonable safeguard against fraudulent and inaccurate financial reporting. 'Financial statements cannot be useful if they are based on unreliable and inaccurate recordings of transactions' (Elmaleh, 2012). Following the financial crisis and the catalogue of public sector scandals, better education and improvements in the transparency of the audit process are needed (ACCA, 2010).

According to Michelson, Stryker and Thorne (2009), Sarbanes-Oxley Act (SOX), Section 404 requires public companies to establish adequate internal controls over financial reporting. Turnbull Report 1999 in the UK provided principle-based guidance for creating strong internal control system and later incorporated into Combined Code, revised in 2005 also presents standalone document on internal controls.

"The application of information technology (IT) has become central to the strategy and business processes of many entities. So, just as IT has become an integral part of the business, IT governance is now seen as an integral part of enterprise governance. In recognition of the importance of IT governance, an IT governance framework, Control Objectives for Information and Related Technology (COBIT) was developed in 1996 as a reference framework for developing and managing internal controls and appropriate levels of security in IT. COBIT provides a set of generally accepted IT control objectives to assist entities in maximizing the benefits derived through the use of IT and developing the appropriate IT governance and control in a company" (IFAC, 2006). While Committee of Sponsoring Organizations of the Treadway Commission, (COSO) in the US and Turnbull report in the UK focus on the achievement of business objectives at the overall entity level, COBIT focuses specifically on information technology. These developments in internal controls issues have created similar developments in some other countries such as Canada, the European Union, Hong Kong, South Africa etc.

Organizations that can survive the currents in the uncertain competitive business environments must, as matter of necessity, 'know how to take advantage of opportunities and counter threats, in many instances through effective application of controls, and therefore improve their performance'. Internal control is, therefore, a vital aspect of an organization's governance system. Thus, internal controls involve putting in place the right kind of internal measures that will enable an organization to capitalize on opportunities while offsetting the threats. An ability to understand risk, manage risk, implemented, and actively monitor risk by the governing body, management, and other personnel is key to taking advantage of the opportunities and countering the threats in order to achieve the organization's objectives (Li, 2012).

Apart from the prevention and detection of fraud, internal controls are put in place to reflect the strength of the overall accounting environment in an organisation as well as the accuracy of its financial and operational records. "Data security failures can cost a company in several ways. Fines for a single incident have reached as high as $15 million. Legal, IT recovery, and other costs can be several times that. Violations of data security laws can lead to increased regulatory oversight. And then there's the damage to reputation" (Drew, 2012).

One main managerial function that centrally is tasked with the business of capitalising on opportunities and offsetting the threats is the role of internal audit. Internal audit as a whole, in essence, can be seen as a special kind of economic control which is concerned with any phase of business activity which may be of relevant to management. ICT has virtually become indispensable part in the operations of any modern accounting and management information systems.Auditing, therefore, involves going beyond the accounting information or financial records to obtain a comprehensive understanding of the operations under review (Chun, 1997). This is done by testing and understanding of the system is required 'to substantiate their opinions and/or provide advice to management on internal controls' (IT Governance Institute, 2007).

1.2. Statement of problem:

Professional Auditors must make judgements based on the knowledge, skills and experience that they have acquired or developed while training, or while working as a qualified professional. Those judgements must also be based on certain ethical values as well as a duty to serve the public interest.Identifying and assessing audit risk is a key part of the audit process. These risks must then be considered when designing the audit plan. A critical emphasis of the procedures of in identifying audit risks is making inquiries of management and Internal Auditors among others within the entity in order to place some reliance on internal controls (Jones, 2009). The objective of these auditing procedures is identifying risks, fraud and errors by testing Internal controls within the entity in order to place some reliance on management assertions.

According to Pine (2011) when determining the extent to which they may rely on Accounting Application Controls, auditors need to consider the extent to which specified controls have been implemented correctly. Information and Computer technology (ICT) has, by necessity, become fundamental part to any modern accounting information

systems. Paper-based audit evidence is giving way to electronic ones in audit engagements. It isan understatement; however, to state that ICT is a high risk discipline due to high level of vulnerabilities and threats. Auditors' responsibility in identifying fraud, however, has now been acknowledged by regulatory standards and the law. Auditing computerised accounting information systems has, therefore, become quite challenging.

It has become, therefore, very vital that auditors show significant competence ICT and become fully aware the impact of contemporary ICT issues on the audit of a client's financial statements, both in the context of how it is used by a client to gather accounting data, process the data and report the resulting accounting information in its financial statements, and how the auditor can use ICT in the process of auditing the financial statements. The level of Skills in information technology has become a great concern for Audit service providers. The auditor's ICT skill is trailing behind the competence required to complete an engagement successfully. Top concerns are how to bridgethe huge skills gap between what the ICT skills expectations of auditors and the status quo.

1.3. Research Questions:

i. Does computerised accounting information systems present audit risk challenges and hence risk to the reliability of Audit report?
ii. Does the training of future accountants and auditors require revolution to reflect the IT competence requirements by the regulatory environment?

2.0. Dimensions of Internal Controls and Auditor's responsibility

Internal Control assessment now has so much to do with Electronic Data Processing (EDP), Computer Information Systems (CIS) auditing, and Information Systems (IS) auditing which are all now considered an extension of traditional auditing (Lovaas and Wagner, 2012). Internal control is a systems put in place to 'keep an organisation on course' towards achieving their set profitable objectives by minimising sudden surprises from errors, fraud, and theft, which may result in risks of assets loss, unreliable accounting information, non-compliance with rules and regulation and similar risks to an acceptably low level, thus, enabling management to deal rapidly and effectively with their associated risk to stay abreast with the more robust economic and business environment in which an entity operates and the shifting competitive advantage (Ratcliffe and Landes, 2009).

International Federation of Accountants (IFAC), (2012), also emphasises that 'one of the best defences against business failure, as well as an important driver of business performance, is having an effective internal control system, which manages risk and enables the creation and preservation of value'. (Ref: Para. 3) of ISA 610 'Using the work of internal auditors' enumerates the objectives of internal audit functions and explains that they vary widely depending on the size and structure of the entity and the requirements of management.

According to Ratcliffe et al (2009), internal controls are fundamental value creation activity that leads to the achievement of an organization's mission by creating value, enhancing, and protecting stakeholder interest and minimising the chances of organizational failures which eventually can and will actually save time and money, and promote the creation and preservation of value. Internal controls, therefore, involve procedures of putting in place the right kind of internal measures that will enable an organization to take advantage of opportunities while observing risks and reducing the threats. Thus, internal controls involve procedural and technical programmes that the auditor must obtain assurance of their efficiency in order to come to appropriate opinion. The technical procedures involved in the audit of financial statements in the private sector and the public sector are very similar. Both adhere to similar auditing standards and undertake similar processes to gain assurance about the adequacy of the underlying controls and systems that support the transactions (ACCA, 2010).

(Ref: Para. 11) of ISA 610 states that'in order for the external auditor to use specific work of the internal auditors, the external auditor shall evaluate and perform audit procedures on that work to determine its adequacy for the external auditor's purposes'. Byrne (2009) categorises adequate internal controls in a computerised work environment into two broad categories. These are: **General Controls** and **Application Controls.**

2.1. General control:

According to Byrne (2009), there are two main controls under General controls which are Logical or technical controls and administrative or procedural controls and the motives behind general controls are to ensure fraudulent activities by staff or external criminals or both are brought to an acceptably very low level. Therefore, the bedrock of general controls is access controls. Access control, a common everyday phenomenon, is a system enabling authorities to control access to areas and resources in a given physical facility or computer-based information system. Access controls are, therefore, put in place for the following purposes:

i. **Preventative Access Controls:** These are systems that make it impossible to access a resource that a user doesn't have rights to access.
ii. **Detective Access Controls:** They are systems that generate alerts when unauthorized access has occurred but don't stop the access from actually happening.
iii. **Deterrent Access Controls:** These don't restrict the access but they make it clear that permission to access the resource is denied.

Categories of General controls:

2.1.1. Administrative control (Procedural control)

Administrative controls are of paramount importance. Administrative controls form the framework for running the business and managing people within and without the organisation. It therefore encompasses physical access controls. Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, Cable locks, etc. (Ratcliffe and Landes, 2009).

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. They inform people on how the business is to be run and how day to day operations are to be conducted. Administrative controls form the basis for the selection and implementation of physical controls and logical controls. Administrative controls have several sub-activities which include: Separation of Duties, Rotation of Job, Need-To-Know or (Least Privilege) and Mandatory Vacations.

i. **Separation of Duties**

According to Ratcliffe and Landes, (2009), Separation of duties is critical to an assurance of effective internal control because of its effect on the risk of errors and inappropriate actions. This method of procedural internal controls ensures that one person cannot compromise the organization's security. Separating the network and work place into functional areas is an example of administrative physical control. Separating out high-risk duties will also help to prevent errors and mistakes. E.g. Programmers shouldn't test their own code. One person should write the code, and another should test it. A security administrator should modify a user's security profile, not the user. The auditor's role is to make sure this procedure is efficient and effective in averting fraud and error.

ii. **Job Rotation**

This internal control procedure ensures that more than one individual can fulfill a particular task within the company. To the auditor, a test of this control is to be satisfied that there is overlap in regards to the jobs being performed and efficient use of resources. This helps in the event that someone goes on vacation and/or passes away because the departure of a key employee can affect the going concern status of the organisation. The Auditor would perform this evaluation to obtain an assurance that knowledge transfer should is arranged, responsibilities reassigned and access rights removed such that risks are minimised and continuity of the function is guaranteed.

Fraudulent activities, also, are more easily identified and corrected with job rotation. Organisations that are efficient can expect to have less audit work undertaken on 'use of resources' than poorly performing organisations. 'It means that at any one time the auditor has a good, all-round understanding of the organisation and can identify early the managerial, governance and financial risks. 'Use of resources' is possibly the most progressive audit framework in the world" (ACCA, 2010).

iii. **Least Privilege –** (Need to know)

Least privilege control is when users are given just enough permission in order for them to do their job. This, also be referred to as a "need-to-know" basis, ensures that critical and confidential information is withheld from those who should not have access to it. The auditor, as part of his internal control assessment, should be able to test the efficiency and effectiveness in order to verify whether or not there is a risk of data integrity due to poor access controls. This can be accomplished through security clearance levels, sensitivity levels, and modes of operation (i.e. - administrator, power user, etc.). This type of internal control works hand-in-hand with technical controls as will be seen below. The Auditor determines the ICT organisation by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision (IT Governance Institute, 2007).

iv. **Mandatory Vacations**

This is where the auditor ensures that staffs performing certain critical functions abide the procedures. You would think that most people wouldn't let any vacation time accrue. This raises red flags of possibility of fraud and corruption and hence a weakness in the internal controls. Job rotation can be implemented more easily with mandatory vacation. Making personnel take vacations helps to identify fraudulent activities. The Auditor will need assurance that these procedures are being followed to obtain reasonable assurance that internal controls are effective (Solworth, & Sloan, 2004).

2.1.2. Logical controls:

According to Olzak (2010),'a logical control, also called technical controls, is another type of general controls that are used to provide access to your organization's data in a manner that conforms to management policies. This includes the enforcement of the principles of least privilege and separation of duties'.Access control based on role definitions is a much better approach when managing user accounts for a company with more than a handful of users. Roles, or jobs, within your organization are defined. Data owners then determine what access each of the roles should have based on data classification and security policies. There are two approaches to implementing roles (Olzak, 2010). Logical security functions include user account management. In order to provide access control to a user, several steps have to be in place to make it work. It is necessary to create a user account with a login and password. Special features have to be in place here as well. For instance, the login account must uniquely identify the person, but it must be part of a standard similar to all other logins. Secondly, the password has to be sophisticated. It must be at least 6 to 10 characters in size; it cannot be a common password, like "password"; it should have upper and lower case letters and also numbers (Garza, 2011). The three bases upon which technical controls are founded are: **Identification, Authentication and Authorisation** (Ratcliffe and Landes, 2009).

i. **Identification:** an assertion of who someone is or what something is. On computer systems in use today, the Username is the most common form of identification and the Password is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate. Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

ii. **Authentication:** the act of verifying a claim of identity.

The auditor should be aware of user verification systems to be able to test and be assured of the integrity of data that is within the accounting system. The first test should be about user authentication. These are measurable physical characteristics that a person can use to prove their identity. There are a couple types of authentication that we need to consider. The different types of methods for authentication are:

1. Something that you know, like a password. The auditor should be able to test the strength, for example, passwords and dynamic password authentication systems.
2. Something that you have, like a secure token or swipe card.
3. Something that you are, like your fingerprint or a facial scan, Biometric scanning or biometric identification can be done through fingerprints, signature dynamics, iris and retina scanning, voice scanning and matching, facial scanning, or DNA or blood matching.

iii. **Authorizationand permissions**

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies (Ratcliffe and Landes, 2009).

A well-structured logical controls audit is critical for the evaluation of management practices, internal control, and, finally, compliance with policy regarding ICT. An appendix to ISA 300 (Redrafted), "Planning an Audit of Financial Statements", states that 'the effect of information technology on the audit procedures, including the availability of data and the expected use of computer‑assisted audit techniques' as one of the characteristics of the audit that needs to be considered in developing the overall audit strategy' (Byrne, 2009).

With regard to technical information security controls, in many financial institutions, the auditor should obtain assurances in the following issues:

i. Confidentiality of data: critical data on systems is only disclosed to authorised personnel.
ii. Availability of data: critical business systems are available at all times when they are required to be and to what extent these systems are protected against all types of threats, e.g., disasters and losses.

iii. Integrity of data: information on critical systems is always accurate, reliable and timely and the strength of controls in place to prevent unauthorized modification to the software, information, or databases (Lovaas and Wagner, 2012).

2.2. Application controls:

Internal Controls begins with ensuring the accuracy, relevance and reliability of accounting information. Basic processing of accounting data is achieved through computer systems ranging from individual personal computers to large-scale enterprise servers. The role of internal control at Application program examination stage is to put procedures in place such that errors and misstatements are reduced drastically at the data recording and entry level into the organisation's accounting information systems. Application controls relate to procedures used to initiate, record, process and report transactions or other financial data. They are specific to a given application and their objectives are to ensure the completeness and accuracy of the accounting records and the validity of entries made in those records. These are manual or automated procedures that typically operate at a business process level and apply to the processing of transactions by individual applications.

Applications therefore refer to the different software embedded in the organisation's accounting information systems with which accounting and financial information is recorded process and reported for decision making. An effective computer-based system will ensure that there are adequate controls existing at the point of input, processing and output stages of the computer processing cycle and over standing data contained in master files. Application controls need to be ascertained, recorded and evaluated by the auditor as part of the process of determining the risk of material misstatement in the audit client's financial statements.

Application controls can be either preventative or detective in nature and are designed to ensure the integrity of the accounting records. Application controls are in three forms**:** input control, process control and output control and contingency controls.

2.2.1. Input control: This is also referred to as programmed control because, **software**, when well prepared, has inbuilt security systems or can be configured such that it will ensure that validity of entry data totals and document counts, as well as data reasonableness, range, manual scrutiny of documents are ensured and have been rightly authorised. When data is input via a keyboard, the software will often display a screen messageif an input check by the application reveals an anomaly, e.g. 'Supplier account number does not exist'.

Validity checks are the most common example of programmed controls over the accuracy and completeness of input are edit (data validation) checks when the software checks that data fields included on transactions by performing:

i. **'Reasonableness check**, e.g. net wage to gross wage, **Existence check**, e.g. that a supplier account exists.
ii. **Format checks** ensure that information is input in the correct form. For example, the requirement that the date of a sales invoice be input in numeric format only – not numeric and alphanumeric.
iii. **Range checks** ensure that information input is reasonable in line with expectations. For example, where an entity rarely, if ever, makes bulk-buy purchases with a value in excess of $10,000, a purchase invoice with an input value in excess of $10,000 is rejected for review and follow-up.
iv. **Compatibility checks(Manual checks)**ensure that data input from two or more fields is compatible. For example, a sales invoice value should be compatible with the amount of sales tax charged on the invoice.
v. **Exception checks** ensure that an exception report is produced highlighting unusual situations that have arisen following the input of a specific item. For example, the carry forward of a negative value for inventory held.
vi. **Sequence checks** facilitate completeness of processing by ensuring that documents processed out of sequence are rejected. For example, where pre-numbered goods received notes are issued to acknowledge the receipt of goods into physical inventory, any input of notes out of sequence should be rejected.
vii. **Control totals**also facilitate completeness of processing by ensure that pre-input, manually prepared control totals are compared to control totals input. For example, non-matching totals of a 'batch' of purchase invoices should result in an on-screen user prompt, or the production of an exception report for follow-up. This total could also be printed out to confirm the totals agree as

output for cross-check. The use of control totals in this way is also commonly referred to as output controls.

viii. **Check digit verification (Character check) i**s process that uses algorithms to ensure that data input is accurate. For example, internally generated valid supplier numerical reference codes, should be formatted in such a way that any purchase invoices input with an incorrect code will be automatically rejected' (Pine, 2011).

These are different checks that the application can be configured to do at input control level. These checks include 'Data input controls ensure the accuracy, completeness, and timeliness of data during its conversion from its original source into computer data, or entry into a computer application. Data can be entered into a computer application from either manual online input or by scheduled automated processing. The input control reviewer or the auditor, in conducting his procedures to understand the IT controls per ISA 315, should determine the adequacy of both manual and automated controls over data input to ensure that data is input accurately with optimum use of computerized validation and editing and that error handling procedures facilitate the timely and accurate resubmission of all corrected data' (Syracuse University, 2012).

2.2.2. Process control: Processing controls ensure the accuracy, completeness and timeliness of data during either batch or online processing of data. Processing controls is built into an application from the development stage through rigorous testing and periodic running of test data.E.g. Running two sample set of parallel data should able to return equal results. Documentation should exist explaining the workflow through the application. Examples would be narratives on the application processes, flowcharts, and an explanation of system or error messages.This is what process controls seek to achieve to ensure the integrity of the application. E.g., the beginning balances on the receivables ledger plus the sales invoices (processing run 1) less the cheques received (processing run 2) should equal the closing balances on the receivable ledger.' These controls will insure that data is accurately processed through the application and that no data is added, lost, or altered during processing (Syracuse University, 2012).

Auditing to ensure system logging system is well-configured is an important skill that is required here. Log files are generated during processing. These logs contain information about each transaction. System Auditing, an addition to traditional financial statements audit, is a way of tracking the occurrence of entrance or attempted entrance into a system. This is important because it shows how successful the access control system is, as well as who was denied, and if they attempt entrance more than once, their intent in getting into the system can be analysed.Processing logs show errors or problems encountered during processing. These logs should be the source for error reports to be used for trend analysis and follow up analysis. "Data that should be included are: who initiated each of the transactions, the data and time of the transactions, the location of the transaction origination (IP address as an example). Logs are used for activity reporting and anomaly detection'. Auditors should be aware of this in understanding the environment of the business in their procedures to assess risks faced by the organisation and the strength of the internal controls.There should be controls in place to document the correct files are used for processing.Processing edits should also be used. These can limit large scale damage which could result in a major database recovery effort" (Elmaleh, 2012).

2.3. Output and contingency controls:

Output controls ensure the accuracy, completeness and security of output. Data output controls ensure the integrity of output and the correct and timely distribution of any output produced. Output can be in paper, an email attachment, as file input to another application or on an online screen. Output controls result in the verification of accurate control totals, and timely result distribution.Measures taken to ensure effective output control include: Investigation and follow-up of error reports and exception reports, Batch controls to ensure all items processed and returned, Controls over distribution/communication/copying output and Labelling of storage disks/tapes. Most output control measures in internal controls coincide with contingency controls.

2.3.1. Contingency control mainly deals with storing, protecting, updating and restoring processed data or other productive resources of the organisation, risk assessment and risk management, as well as reducing nasty and needless interruption of business processes to acceptably low level. "Computerized systems are particularly vulnerable to theft, damage, disruptions, or misuse. The proper use and accounting of information systems depends not only on technical, organizational and design factors but also on the behaviour of people. Computer disasters include theft, virus, malicious damage, hardware faults, hacking,

environment, software, communications, human error or negligence, natural disasters, etc. These disasters affect efficiency and effectiveness of systems and the organisational resources. To remain efficient and effective, organizations have to adopt a proactive approach to manage crisis caused by computer disasters. Proactive approach to crisis management includes forecasting potential crises and planning to deal with them. Generally, organizations have time and resources but they do not have orientations for adopting contingency planning to deal with crises" (Kundu and Jain, 2002). Recent development on Auditing Standards puts a responsibility on auditors for fraud and error detection and therefore the auditor's ability to design procedures to assess the effectives of contingency control measures is imperative. Measures taken under contingency controls include the follow:

Back up/Storage and Filing (Data classification) Controls:

Back up controls aim to maintain system and data integrity. Backup copy of a file is a duplicate copy kept separately from the main system and only used if the original fails. Data stored for a long time should be tested periodically to ensure it is still restorable – it may be subject to damage from environmental conditions or mishandling.

A well-planned data back-up scheme and strategy should include:

i. "A plan and schedule for the regular back-up of critical data.
ii. Archive plans
iii. A disaster recovery plan that includes offsite storage.
iv. There should be documented procedures to explain the methods for the proper balancing/reconciliation and error correcting of output.
v. Output should be reviewed for general acceptability and completeness, including any control totals.
vi. There should be error reports. These should contain:
   - A description of problems/errors and date identified
   - Corrective action taken
vii. Record retention and backup schedules for output files should be established. Consideration should be given to rotate output files offsite" (Syracuse University, 2012).

3.0. Auditors' and responsibility top challenging concerns

International Standards on Auditing (ISA) 240, states that when external independent auditors are performing risk assessment procedures and related activities, to obtain information for use in identifying the risks of material misstatement due to fraud', they should obtain an understanding of the entity and its environment, including the entity's internal control, required by ISA 315 (315 (Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment), that also states that the auditor shall obtain an understanding of the information system, including the related business processes, relevant to financial reporting, including procedures, within both information technology (IT) and manual systems, the auditor obtain an understanding of how the entity communicates financial reports, the auditor shall obtain an understanding of how the entity has responded to risks arising from IT (Byrne 2009).

Audit risk the probability that the auditor will express an inappropriate audit opinion such as the financial statement represents truth and fair state of affairs when the financial statements are materially misstated. Audit risk is a function of material misstatement (control risks and inherent risks) and detection risk.

Control risk involves the risk that 'a misstatement could occur in an assertion about a class of transaction, account balance or disclosure, and that the misstatement could be material, either individually or when aggregated with other misstatements, and will not be prevented or detected and corrected, on a timely basis, by the entity's internal control'.

Inherent risk denotes the risk of 'an assertion about a class of transaction, account balance, or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls'.

Detection risk describes the risk that 'the procedures performed by the auditor to reduce audit risk to an acceptably low level will not detect a misstatement that exists and that could be material, either individually or when aggregated with other misstatements' (Jones, 2009).

Audit risk is fundamental to the audit process because auditors cannot and do not attempt to check all transactions or have the competence to test all the controls thoroughly. Identifying and assessing audit risk is, however, a key part of the audit process, and ISA (315)gives an overview of the procedures that the auditor should follow in order to obtain

an understanding sufficient to assess audit risks, and these risks must then be considered when designing the audit plan. ISA 315 further identifies three risk assessment procedures: Observation and inspection, Analytical procedures, and more relevantly important making inquiries of management and Internal Auditors among others within the entity in order to place some reliance on the controls(Jones, 2009).

Internal audit functions are executive function according to Turnbull report 1999, Sarbanes Oxley Act (SOX) 2002 and Combined Code 2005. It is required to provide audit reports on the effectiveness of their organisation's internal controls, high-level evaluations of governance and risk-management systems. ISA 610 provides guidance on the use of internal audit report. It requires to auditor to consider objectivity, technical competence, due professional care and communication in order to in determining whether or not internal audit report is adequate.

Recent risk management failures reveal a major governance gap in which Internal audit itself needs to be more proactive in pursuing a governance role but credibility is a problem. The auditor, therefore, must be able to rise above just relying on internal audit report. Rather, auditors are expected to proactively be competent enough to test the sophisticated technical controls themselves to reduce risk of misstatement in their audit report. “Norman Marks, vice-president, governance, risk and compliance for Germany's SAP Business Objects division, has said it is a critical time for audit leaders. They need to assess governance and risk-management processes, not just perform audits of controls in specific higher-risk areas” (Swanson 2009).

The Auditor’s responsibilities for detection of fraud are more controversial now than their responsibilities for detecting error. Fraud is an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception with or without external support to obtain an unjust or illegal advantage ((ISA 240 (Redrafted)). ‘Fraud may involve sophisticated and carefully organised schemes, designed to conceal fraudulent activity, such as forgery, deliberate failure to record transactions, or intentional misrepresentations being made to the auditor. However, in order to better understand fraud and error, more consideration of internal control effectiveness is required’ (Jones, 2009). “The traditional ‘passive philosophy’ towards auditor responsibility for fraud detection established in the UK common law tradition, given in the 1896 Kingston Cotton Mill case in which it was held that an “auditor is not bound to be a detective, or… to approach his work with suspicion, or witha foregone conclusion that there is somethingwrong. He is a watchdog, not a bloodhound” has been overridden by the fraud responsibilities in ISA 240 (Jones, 2009).

ISA 200 (Revised and Redrafted), ‘Overall Objective of the Independent Auditor and the Conduct of an Audit in Accordance with ISAs’,requires the auditor to ‘plan and perform an audit with professional scepticism, recognising that circumstances may exist that can cause the financial statements to be materially misstated. It maintain that professional scepticism is‘an attitude that includes a questioning mind, being alert to conditions which may indicate possible misstatement due to error or fraud, and a critical assessment of audit evidence’. Professional scepticism is of key importance to the audit, for example requiring auditors to be alert for audit evidence contradicting other evidence, information questioning evidence reliability conditions that may indicate possible fraud circumstances that suggest the need for audit procedures in addition to those required by the ISAs. Professional Scepticism without the knowledge, skills and experience that they have been acquired or developed while training is not adequate. The auditor should be able to obtain confirmed feedback of his scepticism by being personally able to test the effectiveness of the internal controls.

Outsourcing and reliance on external expert advice may be resorted to but this also complicates inherent and control risks for the auditor and even adds to time and cost of auditing. ISA 620 ‘Using the Work of an Auditor’s Expert’ provides guidance on outsourcing for expert in service ‘in a field other than accounting where, the auditor, who is skilled in accounting and auditing, may not possess the necessary expertise to audit those financial statements. The engagement partner is required to be satisfied that the engagement team, and any auditor’s experts who are not part of the engagement team, collectively have the appropriate competence and capabilities to perform the audit engagement. Further, the auditor is required to ascertain the nature, timing and extent of resources necessary to perform the engagement. The auditor’s determination of whether to use the work of an auditor’s expert, and if so when and to what extent, assists the auditor in meeting these requirements. As the audit progresses, or as circumstances change, the auditor may need to revise earlier decisions about using the work of an auditor’s expert’. (Ref: Para. A38) of the standard states that ‘when an auditor’s expert’s work involves the use of source data that is significant to that expert’s work, procedures such as the following may be used to test that data:

i. Verifying the origin of the data, including obtaining an understanding of, and where applicable testing, the internal controls over the data and, where relevant, its transmission to the expert.
ii. Reviewing the data for completeness and internal consistency.

(Ref: Para. 14) of ISA 620 standard makes it clear that 'the auditor shall not refer to the work of an auditor's expert in an auditor's report containing an unmodified opinion unless required by law or regulation to do so. If such reference is required by law or regulation, the auditor shall indicate in the auditor's report that the reference does not reduce the auditor's responsibility for the auditor's opinion' though subject to (Ref: Para. A41). This means that the use of auditor's expert may be quite risky when things go wrong from the expert's side.

4.0. Findings and recommendations

Internal controls can clearly be seen to have two major dimensions: technical and non-technical dimensions.From the above it is clear that in an audit engagement the distinction between the two types of controls requires considerable dexterity as the two are very often inter-related. Needless to say that the distinction should not be artificially made and administrative controls generally have a more serious connection with the accounting applications controls even if the linkage is indirect (Moorthy, 1999).

Although fraud detection still could be said to be the primary responsibility of management, and those charged with governance, the auditors' role of the auditor and fraud detection responsibility have has still remained a priority of audit standard regarding the current extent of auditor responsibility. ISA 240 enjoins the auditors to design procedures that will enable the auditor to detect material fraud and errors. Hence, both the entity itself and the auditors have responsibilities for fraud and error.

'Internal audit has never been more vital to an organisation than now 'but the challenges to internal audit's influence and credibility have never been greater. The auditor must now report on the adequacy of accounting systems and internal controls more explicitly than for a normal statutory audit" (Collins et al 2012). The requirements for internal control reporting and the procedures by the auditor to verify the strength of the internal controls through the procedures required by ISA 315 to understand the business environment in to order to assess the risks that the accounting information under review is quite complex. The complexity is made even more serious due to the use of technologies in the preparation and presentation of the accounting information. Information technology is traditionally not the field of the accountant even though he is required to apply it in his course of work.Skills gap, therefore, would put pressure on Auditors to outsource experts' hand in these aspects. This, in short, would create a long chain of outsourced personnel on a single audit assignment. Thus, not only would this lead to high audit fees charged, it would also lead to high risk of security of sensitive information and also increase the likelihood of fraud as a result of a likely general control risks (Anomah, 2012).

The current development requires that auditor to be more knowledgeable in the audit of information technology in order to be able to competently complete an engagement on time and cheaply.Training for competence in IT auditing cannot be the preserve of the IT experts alone. Since the information that the external auditor will be needing in auditing and expressing audit opinion is clearly embedded in technology.The auditor's skills in diagnosing IT systems both in software and hardware have become quite critical in these times. As a matter of principle, professional accountants/auditors have the duty to obtain and maintain skills and knowledge required to ensure that clients and trainees receive competent professional service based on current development in practice and in techniques.

Ayeboafo (2012) empirically found that 'Accounting Education emphasizes more on quantitative and decision-making techniques and less on newer developments'. Both formal Accounting Education at the tertiary institutions and professional accountancy training bodies have largely neglected computerized accounting although most organizations are computerizing their accounting with sophisticated cutting edge ICT systems.

It therefore highly recommended now than before that practitioners in the fields of accountancy who have been educated in the key aspects of information technology can bring their experiences to bear in reshaping the design of curricula of accountancy syllabi. Thus, practicing accountants should be made to contribute effectively and efficiently in satisfaction of the increasing ICT requirements of accounting information systems and auditing financial reporting systems in modern organizations.

5.0. Conclusion

The scope of traditional auditing has changed and the change is not only being promoted by regulatory bodies but also by the enactment of legislations. These developments come in the wake of weaknesses in the traditional auditing systems that have resulted in the loss of confidence in profession. The circumstance has become more challenging for the audit profession as the advancement in the use of cutting edge Information and Communication Technology has proved that there is a gap between the current competences of professionals in general and what is required to provide a comprehensive audit according to the regulations and laws.

It has been recommended that practitioner in the fields of accountancy who have been educated in the key aspects of information technology should bring their experiences to bear in reshaping the design of curricula of accountancy syllabi. Practicing accountants should use their rich experiences to contribute effectively and efficiently to satisfy the increasing ICT requirements of accounting information systems and auditing financial reporting systems in modern organizations.

6.0. References

1) ACCA (2010) 'Enhancing External Audit: Learning from the Public Sector' (Discussion Paper), http://www.accaglobal.com/content/dam/acca/global/PDF-technical/public-sector/tech-tp-gf05.pdf (accessed on 09 January 2013)
2) Anomah, S. (2012) Standardising Accounting Information Systems–The Facts and Fads: The Case of Corporate Online Financial Reporting, International Journal of Social Science Tomorrow Vol. 1 No. 10.
3) Ayeboafo, B. (2012). The Role of Accounting Educators in Bridging the Gap between Accounting Theory and Accounting Practice. Research Journal of Finance and Accounting, 2(10), 111-114.
4) Byrne P. (2009), Auditing in a computer-based environment, http://www.accaglobal.com/content/dam/acca/global/pdf/sa_aug09_byrne.pdf(accessed on 29 December 2012)
5) Cai Chun, (1997),"On the functions and objectives of internal audit and their underlying conditions", Managerial Auditing Journal, Vol. 12 Iss: 4 pp. 247 – 250
6) Collins D, Dewing I, Russell P, (2012),"New roles for auditors and reporting accountants in UK banking supervision under the Banking Act 1987", Accounting, Auditing & Accountability Journal, Vol. 25 Iss: 3 pp. 535 - 565
7) Coopers & Lybrand (1994) Internal Control – Integrated Framework, http://www.snai.edu/cn/service/library/book/0-framework-final.pdf, (accessed on 29 December 2012)
8) Drew J (2012), PwC: Internal audit has to play a more substantial role in information security, http://www.journalofaccountancy.com/News/20126231 (accessed on 24 November 2012)
9) Elmaleh M. S (2012) The Reliability and Accuracy of Financial Statements, http://www.understand-accounting.net/TheReliabilityandAccuracyoffinancialstatements.html (accessed on 28 December 2012)
10) Garza G, (2011) Examples of Logical Security, http://www.brighthub.com/computing/enterprise-security/articles/106207.aspx?cid=parsely_rec(accessed on 28 December 2012)
11) IFAC Publications (2006), Professional Accountants in Business Committee International Good Practice Guidance - Evaluating and Improving Internal Control in Organizations, http://www.ifac.org/publications-resources/evaluating-and-improving-internal-control-organizations-0, (accessed on 08 November 2012)
12) IFAC (2012), Effective Governance, Risk Management, and Internal Control, https://www.ifac.org/publications-resources/effective-governance-risk-management-and-internal-control#node-19388 (accessed on 28 December 2012)
13) IT Governance Institute (2007), Framework Control Objectives Management Guidelines Maturity Models, http://khabib.staff.ugm.ac.id/downloads/lecture/ITAudit/COBIT.pdf (accessed on the 09 January 2013)
14) ISA 240 (2010),THE AUDITOR'S RESPONSIBILITIES RELATING TO FRAUD IN AN AUDIT OF FINANCIAL STATEMENTS, http://www.frc.org.uk/getattachment/9ac476b3-bc68-4a87-ac93-bb33fd7dd0e7/ISA-240-The-auditor-s-responsibilities-relating-to-fraud-in-an-audit-of-financial-statements.aspx (accessed on the 30 December 2012)
15) ISA 315 (2010) IDENTIFYINGAND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT THROUGH UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT, http://www.frc.org.uk/getattachment/e87fc063-4e86-4bf0-adec-6ac71db0a349/Clarified-ISA-315-Identifying-and-Assessing-the-Risks-of-Material-Misstatement-Through-Understanding-the-Entity-and-its-Environment.aspx (accessed on 30 December 2012)
16) ISA 620 (2009) 'Using the Work of an Auditor's Expert', http://www.ifac.org/sites/default/files/downloads/a035-2010-iaasb-handbook-isa-620.pdf (Accessed on 01 January 2013)
17) Jones – a - M (2009) ISA 240 (redrafted) Auditors and fraud - And the End of Watchdogs and Bloodhounds, http://www.accaglobal.com/content/dam/acca/global/pdf/sa_march09_jones.pdf (Accessed on 01 January 2013

18) Jones – b - M, (2009) Audit Risk, www.accaglobal.com, student accountant 11/2009.
19) Kundu S. C and Jain D (2002), CONTINGENCY PLANNING FOR MANAGING COMPUTER DISASTERS - A STRATEGIC SUPPORT TO HUMAN RESOURCES IN SOFTWARE INDUSTRY, Delhi Business Review,Vol. 3, No. 2, July - December 2002
20) Li C (2012), 'The Consequences of Information Technology Control Weaknesses on management Information systems: the case of Sarbanes–Oxley internal Control reports', MIS Quarterly Vol. 36 No. 1 pp. 179-203/March 2012.
21) Lovaas P and Wagner S (2012) 'IT Audit Challenges for Small and Medium-Sized Financial Institutions', http://www.albany.edu/iasymposium/proceedings/2012/7-Lovaas&Wagner.pdf (assessed on 04 January 2013)
22) Michelson S, Stryker J and Thorne B (2009), 'The Sarbanes-Oxley Act of 2002: what impact has it had on small business firms?', www.emeraldinsight.com/0268-6902.htm (accessed on 28 December 2012)
23) Moorthy V (1999) Evaluation of Internal Controls with Special Reference to the Audit of Public Sector Enterprises in India, http://www.asosai.org/journal1999/evaluation_of_internal_controls.htm(accessed on 29 December 2012)
24) Olzak T, (2010), Logical/Technical Security Controls - Part 1, http://www.brighthub.com/computing/smb-security/articles/2482.aspx(accessed on 28 December 2012)
25) Pine B (2011), 'Specific aspects Of Auditing in a Computer-Based Environment', http://www2.accaglobal.com/pubs/students/publications/student_accountant/archive/sa_jan11_CAATs.pdf(accessed on 29 December 2012)
26) Ratcliffe T. A and Landes C. E. (2009), Understanding Internal Control and Internal Control Services, American Institute of Certified Public Accountants Inc., (AICPA), New York, NY, 10036-8775.
27) Solworth, J., & Sloan, R. (2004). Security property based administrative controls. Computer Security–ESORICS 2004, 244-259.
28) Syracuse University (2012), Application Self Evaluation, http://amas.syr.edu/AMAS/display.cfm?content_ID=%23%28%28%25%21%0A(accessed on 28 December 2012)
29) Swanson D. (2009), Internal Audit's Identity Crisis, http://www.accaglobal.com/en/student/publications/sa-archive/2009-archive/may-2009/identity-crisis.html, (accessed on 29 December 2012)

This academic article was published by The International Institute for Science, Technology and Education (IISTE). The IISTE is a pioneer in the Open Access Publishing service based in the U.S. and Europe. The aim of the institute is Accelerating Global Knowledge Sharing.

More information about the publisher can be found in the IISTE's homepage: http://www.iiste.org

CALL FOR PAPERS

The IISTE is currently hosting more than 30 peer-reviewed academic journals and collaborating with academic institutions around the world. There's no deadline for submission. **Prospective authors of IISTE journals can find the submission instruction on the following page:** http://www.iiste.org/Journals/

The IISTE editorial team promises to the review and publish all the qualified submissions in a **fast** manner. All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Printed version of the journals is also available upon request of readers and authors.

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar