The impact of INFORMATION SYSTEM SECURITY POLICIES AND CONTROLS ON FIRM OPERATION ENHANCEMENT FOR KENYAN SMES

Ogalo, James Ochieng (PhD)
Full Length Research

The impact of information system security policies and controls on firm operation enhancement for Kenyan SMEs

Ogalo, James Ochieng

Lecturer Kenya Institute of Management (KIM). Email: jamesogalo@yahoo.com, Tel: +254721622234

Accepted 29th May, 2012

The adoption and integration of Information and Communications Technology (ICT) into the business processes is indeed spreading rapidly, firms seek to improve their operations efficiency through increased integration of ICT. Organizations are sometimes skeptical about its absolute adoption in some processes due to complexity of ICT, the impact and security and controls of its integral processes and use. Therefore these studies assessed the impact of information system security policies and control on firms’ operation enhancement with specific objectives of exploration of information system infrastructure security control method, determination of the commonly used information system security control methods and establishment of the effectiveness of ICT management policies by small enterprises (SEs). The study was conducted in Kisumu City (Central Business Districts) in Kenya using survey research design with a target population of 481 of small enterprises firms in Kisumu City Central Business District. The sample population was stratified into two strata namely zone eight and seven and the sample of 144 were selected using purposive sampling method. The sample size was determined according to Yamane (1967) formula for sample size determination. Data was collected through the use of questionnaire and the results presented in tables. From the findings, it became evident that organizations should formulate strategy which should give direction and establish priorities for the investments and management of ICT infrastructure resources. It should complement an ICT governance framework for defining the distribution of the decision-making roles and responsibilities among different levels of managers and employees in the organization, and further establish procedures for implementing and monitoring these strategic decisions. Further constant periodic assessments of ICT risk should be conducted to identify emerging threats that could negatively affect ICT operations and assets utilization.

Keywords: ICT Policies, SMEs, ICT infrastructure

INTRODUCTION

Computer based Information System infrastructure exposes firms’ information resources to a no man’s land where anybody could get access if no proper measures are put in place. These measures should ensure that no unauthorized staff is allowed to access any of the Trust’s computer systems or information stores; as such access would compromise information integrity, also determination of which individuals are to be given authority to access specific information; levels of access to specific systems should be based on job function, independent of status.

Adding to the complexity of information security is the fact that organizations must enable employees, customers, and partners to access information electronically to be successful in this electronic world. Doing business electronically automatically creates tremendous information security risks for organizations. Surprisingly, the biggest issue surrounding information
Security is not a technical issue, but a people issue. (Haag et al., 2008).

The adoption and the use of ICT become one of the options for re-energizing business processes. Fagerberg, et al., (2000) argue that what matters for economic growth is the ability to exploit areas of high technology opportunity, which in recent decades have been dominated by ICT.

Depending on the level of security, removable media used by the staff is disposed of securely and in most cases seeking guidance from the IT Department where appropriate. To ensure consistence and accountability of what get in and out of the system, Checklist for Staff is completed before an employee leaves a job; that relevant accounts are closed and equipment returned for example, mobile phones, PDAs, laptops, and so on.

There exist an increasingly need for adequate ICT control and governance, and is also growing tremendously as firms relentlessly step up the pace and increase the value of return on investments in ICT.

Significance of information system security policies and control

Today, our businesses, governments, schools and private associations, such as churches, are incredibly dependent on information systems and are, therefore, highly vulnerable if these systems should fail. (Laudon and Laudon, 2006). It is therefore obvious that adoption of Computer based Information System requires a high degree of conformance to security policies and control measures by the firm to avert unauthorized access, destruction of the ICT infrastructure and business risks. Such risks include accidental data change or release, malicious user damage, fraud, theft, failure and natural disaster.

The report by Craig et al (2003), confirmed that while the adoption of ICT in businesses of all sizes is predominately high, there has been limited adoption of security practices and technologies. The ABS have reported that only 15% of medium sized firms, 4% of small businesses and 2% of micro businesses have adopted a security policy (ABS, 2003a).

The company needed an advanced threat management solution that would take fewer resources to maintain and require limited resources to track and respond to suspicious network activity. The company installed an advanced intrusion detection system allowing it to monitor all of its network activity including any potential security breaches (CIO Magazine, 2003).

Security and risks of information system resources in general has never been complete and safe at any given time and has to be monitored and evaluated continuously by identifying, quantifying, and prioritizing risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

Background of the study

According to Haag et al (2008) point of view, it becomes undisputable that the technological changes of ICT in terms of emerging trends and technologies are here to stay, those organizations that can most effectively grasp the deep currents of technological evolution can use their experiences to protect the companies against eventual and fatal technological obsolescence. Technology is advancing at a phenomenal pace. Medical knowledge is doubling every eight years. Half of what students learn in their freshman year college about innovation technology is obsolete, revised, or taken for granted by their senior years. In fact, all of today’s technical knowledge will represent only one percent (1%) of the knowledge that will be available in 2050. (Haag et al., 2008).

Adopting ICT is a difficult task for companies of all sizes, whether they are in developed or developing countries. In fact, a lot of management literature focuses on the organizational changes that firms must go through in order to effectively adopt ICT because they change the way firms do business. While the changes may be beneficial in the long run, they often hurt one department and strengthen another. For example, Zhang Hongwei, senior consultant with D’Long International Strategic Investment, comments that “in order to make Enterprise Resource Planning (ERP’s) cost-saving and efficiency-building features work; managers must be willing to take measures that can be anathema in the state-owned sector, such as selling businesses, laying off workers, and changing longstanding vendor relationships. All of this can be tough to do.” (Yinyu, 2004).

Information System security may not be narrowed down as per see, but may also include Careful assessment and reviewing of firms’ ICT needs as part of the overall ICT strategy, drawing up appropriate requirements, detailed evaluation of suppliers, and stringent management policies of ICT operations as a way of mitigating operation risks.

Therefore on success and failure of information technology, O’Brien (2003) asserts that, information system heavily dependent on information technologies, they are designed, operated, and used by people in a variety of organizational settings and business environments. Thus, the success of an information system should not be measured only by its efficiency in terms of minimizing costs, time and the use of information
resources. Success should also be measured by the effectiveness of information technology in supporting an organization’s business value of the enterprise. Information technology and information systems can be mismanaged and misapplied so that information system performance problems create both technological business failures.

So to succeed, companies need information systems that can support the diverse information and decision making needs of their managers and business professionals. As Schwartz and Evans (1997) conclude, conventional wisdom says knowledge is power, but knowledge harvesting without focus can render you powerless. As companies migrate toward responsive e-business models, they are investing in new data-driven decision support application frameworks that help them respond rapidly to changing market conditions and customer needs.

**Statement of the problem**
Information managed through ICT infrastructure is an important resource in terms of organizational strategic positioning and therefore, its protection and control is a very crucial aspect for the firms’ success. Managing information systems technology and corporate data is more difficult in a distributed networked environment because of lack of a single, central point where management can (Laudon and Laudon, 2006).

**The objective of the study**
The general objective of this study was to assess the impact of ICT security policies and controls on firm operation enhancement for Kenyan SMEs. This study sought to achieve the following specific objectives;
- To explore information system infrastructure security control method used by SEs.
- To determine the commonly used information system security control methods used by SEs
- To establish the effectiveness of ICT management policies used by small enterprises

**Research questions**
What are the information system infrastructure security control methods used by small enterprises in Kisumu? What are the commonly use information system security control methods use by small enterprise in Kisumu? Are ICT management policies effectively used by small enterprises?

**Literature review**
**ICT security and policies**
The use and integration of ICT into the business mainstream, has revolutionized and change the business dimension. As noted by Curtis and Cobham (2008), that the impact of information technology has reshaped the types of work involved within organizations. Frequently those with skills for previous jobs do not have the skills appropriate for the new technology. Many organizations have developed policies to provide the retraining necessary to enable employees to move internally. The drive to develop policies is not just the commercial consideration of “fire and hire” as against the costs of retraining.

Despite the massive investments in information technology in the developed economies, the Information Technology impact on productivity and business performance continues to be questioned. Several studies have been conducted and according to the study conducted by (Hammer and Champy, 1993), the real payoffs occur when Information system/Information Technology development and use is linked with the business reengineering (BPR) efforts coming on stream in the 1990s. Keen (1991) further discusses measuring the cost avoidance impacts of IT/IS. For him these are best tracked in terms of business volumes without increases in personnel. At the strategy level he also suggests that the most meaningful way of tracking Information Technology/Information system performance is in terms of business performance per employee, for example revenue per employee, profit per employee, or at a lower level, as one example – transactions per employee.

Integration of the enterprise has emerged as a critical issue for organisations in all business sectors striving to maintain competitive advantage. Integration is the key to success. It is the key to unlocking information and making it available to any use, anywhere, anytime (Kalakota et al., 1999).

**ICT Implementation and Integration**
Martin (1991) points out that faster, better, cheaper does not necessarily mean “quick and dirty”. The need for fast and efficient design and implementation means that time – intensive activities must be automated or, at the very least, supported by appropriate technology.

It was further noted that the world-class enterprise of tomorrow is built on the foundation of world-class application clusters implemented today (Kalakota et al 1999). Effective implementation of information technology would decrease liability by reducing the cost of expected failures and increase flexibility by reducing the cost of adjustment. The business reaction to the environment remains to be the vital determinant for its effectiveness.

Leading-edge telecommunications technology and the internet cannot make organisation move effective unless underlying organizational issues are fully addressed. Old ways of doing business must also be changed to work
effectively with the internet and related network technologies. Such changes in corporate culture and organisational structure are not easy to make. It took several years of hard work and large financial investments for IBM to make its business processes web enabled to convince disparate business units to adopt a “One IBM” mind-set in which everyone uses common tools (Kanter, 2001).

One IT manager estimates that it takes 5 to 10 times more time to reach an understanding and agreement on system requirements and deliverables when the users and developers are in different countries. This is partially explained by travel requirements and language and cultural differences, but technical limitations also contribute to the problem (Ives et al., 1991).

Implementing enterprise system in an organisation/enterprise is like any other change process in a system. According to O’Leary (2000), its implementations fail is believed to be a direct result of lack of top-level management support. Although executives do not necessarily need to make decisions made by project managers. Many problems can arise if projects fail to grab the attention of top-level management. In most companies, executive have the ultimate authority regarding the availability and distribution of resources within the organisation. If executives do not understand the importance of the enterprise system, delays or stoppages are likely to occur because the necessary resources may not be available when they are needed (O’Leary, 2000).

Ethics and policies of ICT
Information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights and obligations. (Laudon and Laudon, 2006).

Ogalo and Nyangara (2011) asserts, that although the government of Kenya has some policies in place, it must continue to foster and play an active role in encouraging and promoting the use of ICT while ensuring that coherent enabling policies. Formulating an intensive national information policy to cater for SMEs up to the village level, to empower their information base and offer relevant knowledge and training on ICT resources. The policy should also contain an organ to link and partner with small enterprise to assess informational needs, business requirements, insecure use of ICT and safety regulation and to avail or indentify for them the source of such information. To include Provision of financial and non-financial incentives to start-up ICT firms; and offer tax incentives to SMEs that buy ICT products and services from local firms, capacity building and skills development in order to attain national socio-economic goals, for the benefit of national and global development (Ogalo and Nyangara, 2011).

An integrated ICT based information systems have become ubiquitous. People a well as organisations have come to depend on them not only for success and survival, but also for the conduct of everyday transactions and activities. Computer systems have invaded nearly every aspect of our daily lives. As information technology advances, it creates a continuing stream of new issues pertaining to those parts of our lives that it impacts. In business arena, information technology has presented ethical issues in four areas these areas, identified by Richard Mason, are privacy, property accuracy and access ( Mason, 1991). In addition, ethical issues surround the impact information technology has on us all.

Curtis and Cobham (2008) found that organizations policy decisions on the use of their IT facilities by employees for non-work- related activities, may cover, for example, the right of the employee to use e-mail for personal purposes, during or outside of work time. The content of the e-mail may also be subject to the policy for example pornography or whether the e-mail is being used for personal consultancy purposes.

Over the last decade, information and communication technologies have enabled changes in the way people live, work, interact and acquire knowledge. The take up of social computing and new participative approaches impact public services such as government, the health sector and education and training (Osimo, 2008; Ala-Mutka, 2008; Punie, 2008; Redecker, 2008).In another study of African and Latin American nations, Wallsten, (2001) observed that regulation had no impact on mainline telephone penetration. The prevailing individual nation conditions (economic, cultural, social, and political) also should be considered when investigating ICT adoption in African nations.

ICT policy making in developing countries may suffer from weaknesses (Maclean et al., 2002). Involving the business sector can help overcome those gaps. However, the most important role of the business sector is to supply to the market, local innovative solutions that can respond to local specific needs thus diffusing ICT.

Information security and ICT governance
Business enterprises have very valuable information assets to protect. Systems often house confidential information about individual’s taxes, financial assets, medical records and job performance reviews. They also may contain information on corporate operations, including trade secrets, new product development plans; systems may store information on weapons systems, intelligence operations, and military targets. These information assets have tremendous value, and the repercussions can be devastating if they are lost,
destroyed, or placed in the wrong hands. A recent survey estimates that when the security of a large firm is compromised, the company loses approximately 2.1 percent of its market value within two days of the security breach, which translates into an average loss of $1.65 billion in stock market value per incident (Cavusoglu et al., 2004).

Issues such as perceived investment recovery, comfort with traditional forms of supply management and selling, perceived levels of risk, security concerns and training costs are cited as being serious barriers to uptake of ICT by SMEs (Kendall, 2001).

Effective security management can minimize errors, fraud, and losses in the internetworked computer-based systems that interconnect today’s e-business enterprises. (Tate and Priscilla, 1998). Companies have very valuable information assets to protect. Systems often house confidential information about individual’s taxes, financial assets, medical records, and job performance reviews. They also may contain information on corporate operations, including, trade secrets, new product development plans and marketing strategies. Government systems may store information assets that are on their own tremendous value, and the repercussions can be tremendous, and the repercussions can be devastating of they are lost, destroyed or placed in the wrong hands. A recent study estimates that when the security of large firms is compromised, the company loses approximately 2.1 percent of its market value within two days of the security breach, which translates into an average loss of $1.65 billion in stock market value per incident (Cavusoglu et al., 2004).

Defrauding telephone companies out of long-distance toll charges has occurred for many years. Using slugs instead of real coins, letting the phone ring twice to mean you go home ok, and calling person-to-person for yourself with some cute message are all ways that people have swindled common carriers out of toll charges that were rightly theirs (Emma, 1997).

STUDY METHODOLOGY
The study was conducted in Kisumu City, headquarters of Nyaraza province, in the western part of Kenya and is also the third largest City in Kenya. Kisumu is a Lake Victoria port of Kenya and the second most important town after Kampala within the lake region. It is known for it being economic hub for most trade conducted in the East Africa region. Kisumu has an estimated population of about 665,018 people, of whom 162,354 are male and 160,380 Female. (Kenya National Bureau of statistics, Kenya Population Census, 1999).

The study was based in Kisumu city Central Business Districts (CBDs), which is divided into two zones namely; zone seven (7) and zone eight (8), according to Municipal council of Kisumu (MCK) way of classification. Survey research design was used in the study with a target population of 481 of small enterprises in Kisumu City Central Business District. The population was drawn from the sample list from Municipal Council of Kisumu (MCK) integrated information system (MCK integrated information system, 2010). The small enterprises according to the study are enterprises with employees between 5 and 20.

A sample of 144 small enterprises were respondents selected from the target population of 481, and distributed in 310 and 171 respondents respectively in each sub-group named zone 7 and 8, using stratified sampling technique. The sample size was determined according to Yamane (1967:886) formula for sample size determination. The sample for the study was selected from the two strata using purposive sampling technique. Table 1

Purposive sampling technique was further used to select 5 directors of small enterprises for in-depth interviews. The informants were selected at the researchers discretion based on general set up of the ICT use in order to shed light on a range of issues of interest to the study. Also interviewed were ICT professional dealers who were selected using purposive sampling method.

In the study open and closed ended questionnaires and interviews were the main tools used to collect data. But the large sample size of 144 respondents used in this study against the time constraints made of questionnaire the ideal tool for collecting data within the shortest time possible. The study used self administered questionnaire.

To ensure reliability of the instruments, 10% of the instruments were piloted in the small enterprises outside the CBDs; this in correcting some of the error in the instruments, thereby improving instrument reliability.
Reliability is a measure of the degree to which a research instrument yields consistent results or data after repeated trials (Mugenda and Mugenda, 2003).

This pilot testing of the questionnaire improved the content validity of the instrument, by realigning and adjusting the questions to conform and improved its clarity to the respondents. Opinions of the experts were also sought to make the instrument yield the expected results. The data collected were coded, tabulated and analysed using descriptive analysis for measures of central tendency and inferential analysis method to draw conclusions concerning relationships and differences found in the research results.

**DATA PRESENTATION, ANALYSIS, RESULTS AND DISCUSSIONS**

In order to explore further to determine the security policies in the small enterprises, surveyed respondents were asked to indicate if there exist the required levels of security. Results showed that 129 (90%) of the respondents have the required security level which were the overwhelming majority. Only 10 (7%) were for non existence of the required security level, while 5 (3%) decide to remain neutral and therefore did not comment on the same. This supports the fact that most enterprises have existing security level policies in place, because 90% of the respondents were in support. Management of implementation and effective control of security policies poses a serious challenge to most firms. Laudon and Laudon (2006), confirmed that many firms lack disaster recovery and business continuity plans or fail to patch their software routinely against security vulnerabilities. Managers do not appreciate the value of a sound security strategy. Security threats abound, but they are neither predictable nor finite, making it more difficult to calculate returns on security investments. Table 2.

The results show that majority 58 (40%) of the small enterprises strongly disagree that the ICT protection policies were effective. Another 41 (28%) disagree with the same, while 7 (5%) did not choose any side but decided to remain neutral. The remaining 13 (9%) and 25 (17%) were of the opinion of strongly agree and agree respectively. This data was further subjected to likert scale rating, and the value stood at 2.3, above neutral value of 2, and this indicates that ICT protection policies still stands in the middle and a lot has to be done to improve its effectiveness. Table 3.

Good information architecture includes a strong information security plan, along with managing user access and up-to-date antivirus software and patches. (Martin, 2005). The effectiveness of information system security require a rigorous training and sensitization of staffs, to shield some of the obvious loophole which in turns creates a liability to the enterprise.

Many individuals freely give up their Passwords or write them on sticky notes next to their computers, leaving the door wide open intruders. (2002 CSI/FBI, 2003). A detailed information security plan can alleviate people – based information security issues. An organization should make a conscientious effort to ensure that all users are aware of the policy through formal training and other means.

Majority of the respondents according to the above table shows that 99%, 97% and 88% used physical restriction to access critical ICT component, backup power unit and training of employees on current ICT needs and requirement respectively. Some respondents constituting of 19%, 2% and 30% used firewalls, data encryption and data backup as information system protection security facilities respectively. Table 4.

Many U.S firms such as banks and brokerages are required by federal law to provide their customers a copy of their firm’s privacy policy. It is therefore a fundamental responsibility for managers who own or use information resources to protect and secure these assets from theft, damage and misuse. IT managers are expected to lead in establishing IT control policies for the entire firm. (Frenzel and Frenzel 2004). The understanding of managers on the various security protection facilities was an important element for the successful utilization and management. It was further noted that Control also means that managers must have routine methods for comparing actual and planned performance. In a well-controlled organization, deviations from planned performance stand out and are obvious. “Planning and control are inseparable – the Siamese twins of management” (Harold Koontz and Cyril O’Donnell 1964). Frenzel and Frenzel (2004) noted that to cope

### Table 2: Existence of ICT security policies.

<table>
<thead>
<tr>
<th>Details</th>
<th>No. of respondents n=144</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>129 (90%)</td>
</tr>
<tr>
<td>No</td>
<td>10 (7%)</td>
</tr>
<tr>
<td>No Comment</td>
<td>5 (3%)</td>
</tr>
<tr>
<td>Total</td>
<td>144 (100%)</td>
</tr>
</tbody>
</table>

Source: Survey data

### Table 3: Effectiveness of ICT infrastructure protection Policies

<table>
<thead>
<tr>
<th>Details</th>
<th>No. of respondents (Enterprises) n = 144</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>13 (9%)</td>
</tr>
<tr>
<td>Agree</td>
<td>25 (17%)</td>
</tr>
<tr>
<td>Neutral</td>
<td>7 (5%)</td>
</tr>
<tr>
<td>Disagree</td>
<td>41 (28%)</td>
</tr>
<tr>
<td>Strongly Disagree</td>
<td>58 (40%)</td>
</tr>
<tr>
<td>Total</td>
<td>144 (100%)</td>
</tr>
</tbody>
</table>

Source: Survey data
Table 4: Information system protection security facilities.

<table>
<thead>
<tr>
<th>Security method</th>
<th>No. of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls n=144</td>
<td>27 (19%)</td>
</tr>
<tr>
<td>Data Encryption n=144</td>
<td>3 (2%)</td>
</tr>
<tr>
<td>Data backup n=144</td>
<td>43 (30%)</td>
</tr>
<tr>
<td>Physical restriction to access critical ICT components n=144</td>
<td>141 (99%)</td>
</tr>
<tr>
<td>Backup power unit n=144</td>
<td>139 (97%)</td>
</tr>
<tr>
<td>Training of employees on current ICT security needs and requirements n=144</td>
<td>88 (61%)</td>
</tr>
</tbody>
</table>

Source: Survey data

Table 5: ICT infrastructure disruption encountered

<table>
<thead>
<tr>
<th>ICT Disruption</th>
<th>Yes</th>
<th>No</th>
<th>No comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sabotage (Vandalism, Theft) n=144</td>
<td>43 (30%)</td>
<td>68 (47%)</td>
<td>33 (23%)</td>
</tr>
<tr>
<td>Unauthorized Access n=144</td>
<td>86 (59%)</td>
<td>40 (28%)</td>
<td>18 (13%)</td>
</tr>
<tr>
<td>Data loss n=144</td>
<td>121 (84%)</td>
<td>19 (13%)</td>
<td>4 (3%)</td>
</tr>
<tr>
<td>ICT abuse (Fraud, Crime) n=144</td>
<td>56 (39%)</td>
<td>77 (53%)</td>
<td>11 (8%)</td>
</tr>
<tr>
<td>Hardware failure n=144</td>
<td>125 (87%)</td>
<td>16 (11%)</td>
<td>3 (2%)</td>
</tr>
<tr>
<td>Software failure n=144</td>
<td>131 (91%)</td>
<td>8 (6%)</td>
<td>5 (3%)</td>
</tr>
<tr>
<td>Virus attack n=144</td>
<td>140 (97%)</td>
<td>3 (2%)</td>
<td>1 (1%)</td>
</tr>
<tr>
<td>Interruption of telecommunication links n=144</td>
<td>131 (91%)</td>
<td>7 (5%)</td>
<td>6 (4%)</td>
</tr>
</tbody>
</table>

Source: Survey data

successfully with these challenges, effective managers must develop a discerning awareness and a keen appreciation of social phenomena, and they must continually fine tune their people management skills. High performance organizations always find ways to maximize human productivity. They recognize that people are the key to capturing the benefits of technological advances in today's information age.

Table 5 above shows that majority of small enterprise 47% do not experience sabotage as a disruption of ICT operations. About 30% have encountered sabotage, while another 23% decline to comment. On unauthorized access, majority of the firms' 59% have encountered this problem and 28% have not, while only 13% decline to comment. Data loss has a majority of respondents 84% encountering this problem and 13% have encountered the same and 3% declining not to comment. ICT abuse was represented by 39% and 53% respondents citing it as a hindrance to the smooth operation of the system. Hardware failure has a majority of 87% of respondents recognizing it as a problem and 11% do not, while only 2% declined to comment.

The results showed above gives elements of existence of gaps of hindrance of ICT between ICT-disruption related effects and the continuity and maximization of ICT resources. Porter (2001) asserted that new technologies trigger rampant experimentation, by companies and their customers, and the experimentation is often economically unsustainable. As a result, market behavior is distorted and must be interpreted with caution (Porter, 2001). This raise a lot of questions to be solved by management of an enterprise, this necessitates the prioritization of strategic action plans to focus on these problems, the focus should be holistic in nature and not thinking that IT governance, policies implementation and related problems is a restricted responsibility of other reserved people in the organization. This will ensure that the organization is driven to provide proactive leadership to enhance the organizational achievement of the many benefits of optimizing IT opportunities while protecting against risks. It was further noted, that in turbulent times, an enterprise has to be able to withstand sudden blows and avail itself of unexpected opportunities. This means that in turbulent times the fundamentals must be managed and managed well. (Drucker, 1980). It was noted that one problem with risk assessment and other methods for quantifying security costs and benefits is that organizations do not always know the precise probability of threats occurring to their information systems, and they may not be able to quantify the impact of such events accurately. (Mercuri, 2003).

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Summary
The culture of good Internal ICT Control should be inculcated in the entire workforce, which in turn engage the employees and create a sense responsibility,
accountability. This essentially creates adequate procedures, information and channels of reporting amongst others, and coupled with proper documentation of the same for ease of integration in the business system.

Conclusions and Recommendations
Organizations should formulate strategy which should give direction and establish priorities for the investments and management of ICT infrastructure resources. It should complement an ICT governance framework for defining the distribution of the decision-making roles and responsibilities among different levels of managers and employees in the organization, and further establish procedures for implementing and monitoring these strategic decisions.

Constant periodic assessments of ICT risk should be conducted to identify emerging threats that could negatively affect ICT operations and assets utilization.

Information system utilization and security policy and procedures should be developed in a clear terms of reference for its protection and the management of data held in the system should conform and adhere to the set rules and regulations.

REFERENCES
Bureau of Statistics.
Ogalo JO, Nyangara CA (2011). Impact of Information Communication Technology (ICT) on growth of Small


Redecke C (Forthcoming). Review of Learning 2.0 Practices. IPTS technical report prepared for publication.


