CORRUPTION PREVENTION GUIDELINES ON ICT SYSTEMS IN THE PUBLIC SECTOR

Prepared by:
Kenya Anti Corruption Commission
Directorate of Preventive Services
March 2008

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CEO	Chief Executive Officer
CD	Compact Disc
ICT	Information and Communication Technology
ID	Identity
I T	Information Technology

INTRODUCTION

The Government has made great strides in the implementation of e-government in most of its Departments. This has significantly contributed to efficiency in delivery of services. Processes which previously had several steps are now completed instantaneously. There is quick access to information which was previously difficult and time consuming. This is because large databases with networked access have been created. Of significance is the access to various documents required in processing permits such as Passports. In addition, application for jobs in the public service and access to results of national examinations is currently possible electronically. Thus implementation of ICT systems in the public sector has facilitated faster delivery of services. This is achieved through enhanced communication to staff and clients.

Computerization in some government institutions is being hampered by resistance of some officials. This is because many organisations do not take their employees through the change process to allay the fear of computerization. There is also fear of losing jobs because certain tasks can be performed by fewer staff after computerization. As such in most organizations computerization exists hand in hand with manual operations.

Introduction of Information Technology into the public sector has provided new challenges. Furthermore, the shift into IT in the Public Sector has brought about profound opportunities for corruption. Introducing new technologies quickly for functional and fiscal purposes implies that risk assessment and control with regard to e-corruption is not adequate. Lack of installing proper controls and adequate safeguards in the computer systems has provided greater opportunities to IT – literate staff to engage in electronic malpractices.

The Kenya Anti- Corruption Commission, Directorate of Preventive Services, has identified some generic loopholes in Computer Systems while undertaking some of its activities such as systems reviews of public institutions. These loopholes are being used to perpetrate electronic corruption and other economic crimes. The identified loopholes have resulted from poor monitoring of the implementation of IT projects and failure to critically analyse the feasibility of the projects before approval.

This guideline highlights some of the malpractices and makes recommendations to enhance integrity in the management of IT in the public sector. KACC hopes that

the guidelines will contribute to raising awareness on the areas vulnerable to corruption and create the need for an integrated risk management approach to e-corruption.

LOOPHOLES AND INEFFICIENCIES

ICT POLICY

The government developed a national ICT policy in 2006. The policy is based on four guiding principles namely:

- Infrastructure development
- Human resources development
- Stakeholder participation and
- appropriate policy and regulatory framework

An ICT policy provides the framework for developing and maintaining an effective information technology environment. Some of the organizations examined are not aware of the National ICT policy and have continued to implement ICT systems without referring to the policy. This has exposed organizations to serious vulnerability to information systems security violations.

As regards electronic security, the policy focuses on establishing adequate legal framework and capacity to deal with national security, network security, cyber-crime and terrorism and to establish mechanisms for international cooperation to combat cross-border crimes.

IT GOVERNANCE

The pervasive use of technology has created a critical dependency on IT that calls for good IT governance in preventing corruption. IT governance should be spearheaded by Chief Executives and Managers to ensure that the objectives of their respective organizations are achieved.

Many managers are not knowledgeable on IT. Hence they may not identify possible risks even to themselves. They become overly dependent on their IT specialists and may merely rubber stamp the IT managers' proposals. Others depend on outside experts without subjecting their work to quality checks that they can impose to other suppliers. IT officers may take advantage of the situation and, in collusion with suppliers, exaggerate the prices of IT goods and services. In one organization, an IT officer procured services for data recovery over the weekend and although this was not successful a fee note of a substantial amount was presented to the CEO. In an another instance, when KACC team enquired about offsite back-up there was

conflicting response as the IT officer said that the organization had an offsite backup but the CEO was not aware of this.

Where partnership arrangements have been entered into, organizations may fall prey to the partner and become unable to control the operations of the partner institution. Organizations may therefore be unable to control their software and data. Some of the staff from the partner organization could easily facilitate corrupt practices by manipulating data. This has been noted among Local Authorities which have entered into revenue collection contracts that will run for as many as ten years.

The discretion in making IT decisions leads to loopholes that could occasion loss of resources, abuse and manipulation of data and systems for personal gain. Such malpractice could go undetected for a long time.

IT PROJECT MANAGEMENT

Many public organizations do not have formal procedures for classification, planning, execution and monitoring of IT projects. It has been observed that Most public organizations do not carry out feasibility studies before project initiation. Feasibility studies are a necessary prerequisite in the implementation of IT systems. The studies assist organizations in making critical decisions on the nature and size of information to computerize, the appropriate systems necessary to support the data and the sustainability of the system. It also helps in determining areas for networking in order to achieve the intended result.

Lack of proper planning and analysis in terms of cost, business and technical viability has also led to acquisition of over-priced IT Systems and in certain situations near obsolete software. This situation opens loopholes for corruption as the organization may be duped into acquiring unnecessary equipment. This situation exists in some of the public organizations that have been examined by the Commission.

Some of the IT systems reviewed did not have appropriate systems and security control to prevent computer malpractices. Introduction of IT in organizations is supposed to prevent corruption by eliminating the manual processes which are prone to corruption and reducing the human interaction between public officers and the public, this perception is fed into the process of planning new information system and necessary controls may be intentionally omitted when designing systems to safeguard corrupt incomes. For instance, there is a local authority which has a system for revenue collection that did not have audit trails and standard access controls mechanism.

IT OPERATIONS RISK MANAGEMENT

While computerization provides undoubted benefits, it also carries substantial risks to financial and information security. Computerization changes not only how things are done but also the risks they embody. Risks exist wherever a computer is used and where technical or managerial safeguards are lacking. Automation entails reorganizing the processes of performing organizational functions. The faster the process of automation the less it is that the ramifications of the change have been considered. Inadequate risk planning leads to increased future costs where security measures are only incorporated afterwards.

Risk management is the process that allows IT managers to protect the IT systems and data in the organization. This is achieved through preventive control which is meant to inhibit attempts to violate IT Systems security and detective controls to warn of violations or attempted violations of IT Systems security. Inappropriate Risk Management practices result to violations of IT Systems and manipulation of data to facilitate corrupt practices. Below are some of the generic weaknesses found in various public sector organizations

i) Access Controls and User ID Management

User accounts and passwords are allocated to users to identify themselves for the purposes of accounting, security, logging and resource management. IT Systems in most public organizations lack adequate access controls. Some of the weaknesses identified in regard to access controls include:

a) Sharing of passwords and user names resulting to lack of accountability incase of any malpractice in IT Systems.

b) Maintaining Dormant User Accounts in the system which could be used for fraudulent activities.

c) Systems failure to disable user accounts after several unsuccessful login attempts, which makes the system vulnerable **to penetration** by unauthorized persons.

d) Failure to make it mandatory for users to change their passwords after a period of time. Long interval between passwords change in applications increases the risk of compromising passwords security as they become more widely known over time.

e) Default user accounts usually set by software vendors for example the 'administrator' account in windows are still active and have not been renamed.

Unauthorized users may easily gain access into the Computer System using the default accounts since the default passwords are similar.

ii) Systems security monitoring and administration

In many organizations the task of administering security over the computer installations has not yet been assigned. There is no monitoring of significant processing deviations. The number of access attempts is not restricted. Unauthorized access attempts are not monitored. There is no time-out facility when the system is not being used after a pre-determined period. This has resulted to fraudulent activities in the IT Systems going undetected for a long time. More so, it increases the risk of damage to the confidentiality and integrity of the organizations' systems and data.

iii) Separations of duties

In some organizations it was observed that there is no separation of duties between IT operations and other departments like Finance. For instance, in some organizations the IT Administrator can perform tasks in the Finance Department. Failure to separate duties may result to IT Administrators perpetrating fraudulent activities in IT Systems since there is no proper accountability in the functions allocated. The situation is worse in cases where there are no Audit trails in the system or the audit trails are monitored and administered by the same IT Administrator.

Some of the common malpractices found that may occur due to poor risk management include:

a) Manipulation of data

In 2007, KACC examined a public institution that manages a payroll of over 170,000 persons, payments were being made through electronic funds transfer and the institution had to take payroll data to various banks in soft copy to effect funds transfer. Recipients indicated that sometimes they detected changes in their monthly payments. Soft copy of the payrolls distributed to various banks was not encrypted and was stored in diskettes which made it easy for corrupt officers to manipulate the data before being taken to the banks.

b) Printing of parallel receipts (forgery)

In one of the Local Authority, a company was contracted to develop a system for revenue collection. The system was also being used to print various permits issued by the Local Authority. Employees of the

contractor in collusion with some cashiers were issuing forged receipts and permits since they were not serialized and did not have any security features.

BACK UP PROCEDURES

Many organizations do not have backup procedures of their Computer Systems. Although some of the organizations take back ups of their applications, the back ups are stored in the same computers hard disk. Some of the organizations take their backups in tapes but are also stored in the same building. It was also observed that some organizations do not have backups of their data at all. This has resulted to loosing confidential and vital data as a result of systems crash which may be deliberate or may have resulted from vandalism of computer hard disks with the intention of concealing malpractices.

DISASTER RECOVERY AND CONTINUITY PLAN

Disaster Recovery Plans help organizations in recovering normal operations in case of a disaster that may affect a computer room and other IT equipment. A continuity plan is useful in addressing logistical issues, procedures and steps to be adopted by management or individuals in an organization incase of a disaster. Continuity planning involves identifying and reducing the risks from deliberate or accidental threats to vital services.

Many public sector organizations do not have Disaster and Continuity Plans. This makes it difficult for organizations to quickly resume their normal operations after systems crash or other disaster. Prolonged systems breakdown negatively affects service delivery to the public. In such circumstances, organizations are forced to revert to manual processes which are slow and prone to corruption, at times members of the public are extorted by corrupt officers for their cases to be fast tracked in manual system which is slow.

SAFEGUARDS AGAINST CORRUPTION AND INEFFICIENCIES

In order to address the above inefficiencies and malpractices in the management of IT systems in the public sector, it is recommended as follows:-

Dissemination of National ICT Policy

The Ministry of Information and other Government Arms dealing with IT should disseminate the ICT policy. The policy should address the global e-Government strategies and safeguards necessary to prevent e-corruption. The Ministry should create more awareness on the policy to public institutions. Compliance with the policy is imperative and hence the policy should be clearly disseminated to Public Sector employees. This can help identify and minimize the risk of security breaches

Institutional ICT Policy

Due to the unique nature of the functions of Government Departments, it is necessary for each Department to develop ICT policies in line with the National Policy. The policies should stipulate disciplinary action against a member of staff involved in malpractices. This should be in addition to the penalties described in the Anti-corruption and Economic Crimes Act 2003. In addition, the policy should create frameworks for arbitration when contracted firms breach the terms of the agreement. There should be capacity building for officers on how to develop the Policy in line with their business functions. The Executive management should be responsible for overseeing and approving the development, implementation and maintenance of the organizations IT policy.

Organizations should also ensure that that all employees have to sign up to security policies, in particular those governing e-mail, Internet usage and Management Information Systems used in the organization. Appropriate budgetary provisions should be made for training of Chief Executives, Managers and other staff on their roles in IT.

Role of Senior Management

Chief Executive Officers and Senior Management in the Public Sector should make IT governance an integral part of corporate governance and ensure that:

- IT operations are aligned to the organizations' objectives
- IT budget and investment plan is realistic and integrated into overall financial plan
- Organizational structures and responsibilities are setup to facilitate IT strategy implementation.

- There is assurance of the performance, control and risks of IT and independent comfort about IT decisions.

The Executive management should be very clear about its own responsibility and that of IT department in IT governance. The executive management should have a system in place to enforce those responsibilities which generally relate to alignment of IT with the organization's goals and objects, the management of technology-related business risks and the verification of the value delivered by the use of IT in the organization. Due to the importance of IT in organizations, the senior most IT Manager should report to the higher level, preferably to the Chief Executive to proactively increase IT value contribution to the organization and effectively implement an IT control framework.

Information Technology Services outsourcing does not mean consultant dependence. In addition to conducting assessments, preparing risk profiles, and designing management procedures, consultants should be required to transfer skills to a level which ensures effective security management. The Chief Executives and managers should have good contract management skills and basic understanding of the services provided by the consultants. Contract management skills in the public sector and in particular at the Local Authorities are generally poor.

Feasibility studies

Feasibility studies determine the path that should be taken when approaching the development of an IT system. When evaluating alternative approaches it should be noted that development costs can be provided in terms of different estimates based upon the development approach chosen. Therefore, unless the development approach is taken from the outcome of the feasibility study the manpower estimates will be inaccurate, which is the basis for making informed decisions on the choice of the systems.

Organizations should therefore undertake adequate feasibility studies including cost benefit analysis to determine the viability of various options. This will ensure that resources are not wasted. Lack of such analysis results into misallocating resources into an economically or technically unviable project and may also result in termination of the project at an advanced stage after considerable expenditures have already been incurred.

The feasibility study should be the main component that should be used for determining if the Computer project should be approved for development.

Guidelines on Project Management

In order to ensure IT projects are properly managed, all projects should adhere to pre-determined standards and guidelines. A formal policy should be designed to ensure that all projects follow a standard process of classification, planning, execution and monitoring. The project management methodology should, at a minimum, include:

- Classification and prioritization of projects in line with organization core mandate and function;
- Thorough and documented business and technical analysis of the project. (to be used as the basis of management authorizing initiation of the project);
- Risk management plan that will ensure internal and external projects risks are identified and assessed, reported and monitored, and appropriately managed.
- A baseline project schedule with milestones and task responsibilities; and
- A process for tracking and reporting of project progress, task changes, deliverables completion, issues resolution, resource availability, scope and timescale changes.

Systems Audit

In order to ensure that systems control and security requirements have been appropriately incorporated in the systems under development, independent Information Systems Auditors should be used to test controls during development and after implementation of the projects. This will also ensure quality of phase deliverables in the projects.

User ID and password management

In order to address security weaknesses and risks that may lead to abuse, the following should be put in place in the public sector computer systems:

- Every user should have personal user accounts and password

- All user accounts should be reviewed periodically to determine that they are still required. Whenever disabled or stale accounts are identified, they should be removed.

- After three invalid login attempts the user ID should be frozen until the system administrator re-enables it. Requests for re-enabling user

ID's should be investigated by the IT administrator for potential misuse.

- The IT Administrator should obtain authority from the Human Resources Administrator who has a record of all employees to open user accounts. Organizations should also develop access authorization forms to be signed by employees. The forms should inform employees of their responsibility as far as the use of the Computer Systems is concerned and disciplinary action to be taken incase of illegal activities perpetrated in the Computer System.

- Computer Systems should have mechanisms that will force users to change their passwords regularly. Systems which have the mechanism of enforcing change of password settings should be enabled and passwords for critical Systems like Financial Accounting systems passwords should be changed more frequently.

- Default user accounts in Computer Systems should be renamed to other values and where passwords have been supplied to the default accounts the password should also be changed.

- A minimum password length of at least 6 characters should be used and at least 8 characters in critical applications

- Staff should be trained on security awareness regularly. The training should cover issues of systems access control and how to avoid divulging of confidential information regarding their user names and passwords information to hackers through social engineering.

Supervision

Organizations should appoint a member of staff to carry out at least the following functions on a regular basis:

- Review daily history logs for any system warnings or messages.

- Regular maintenance of password file to ensure that all users in the system are authorized staff and passwords are changed on a regular basis.

- Monitoring of unauthorized access attempts.

Additionally the Management should investigate the practicality of a time-out facility after a pre-determined period of inactivity

Separation of duties

There should be segregation of duty between the IT Personnel and the Financial Accountants. IT personnel should only be involved in IT operations and not any financial related functions.

Systems backup

Organizations should develop backup procedures. They should periodically take full back ups of the critical systems, for instance, on weekly basis and then take incremental or differential back ups on daily basis. Desktop Computers and Laptops on a networked environment should be reconfigured to enable automated backups to take place daily onto the server. Full back ups should be a complete copy of the system and where organizations consider incremental backups, such back ups should reflect the changes made since the last back up. Back ups should be taken on removable media like CDs, Tapes and stored offsite. Where possible the organizations critical servers should have an offsite disk mirroring. Departments may consider reciprocal arrangements for offsite backup storage in order to minimize cost.

In cases where confidential and critical data is in a stand alone computer, the Computer hard disk should be encrypted using various hard disk encryption tools or even open encryption tools like True Crypt which can be downloaded from the internet free off charge. This will ensure data security in the event of theft of vandalism of the hard disks.

Disaster Recovery and Continuity Plan

There is need to develop a module to guide organizations on how to develop a Disaster and Continuity Plan. Disaster Recovery plan should put into consideration asset criticality including those of the IT Systems and Data, alternative critical organization processes, back-up and recovery procedures and regular testing of the plan. The staff should also be trained on their individual roles in the plan incase of a disaster.

The Disaster and Continuity Plan should cover the following processes:

- Identification and prioritization of critical business processes by undertaking a Business Impact Assessment.

- Determining the potential impact of various types of disaster on business activities.

- Identifying and agreeing all responsibilities and emergency arrangements in terms of costs to be incurred based on the market rates.

CONCLUSION

The e-governance secretariat was initiated by the government to promote use of ICT to improve service delivery. Although ICT can be used to prevent opportunities for corruption, the implementation of IT projects has demonstrated that ICT can also be used to perpetrate irregularities. Such irregularities stem from faulty procurement process to failure by suppliers and vendors to honour contractual agreements. As a result some IT projects within the public sector fail after substantial resources have been expended. Malpractices in the implementation and sustainability of ICT within the public sector may threaten the gains that the Government is making through computerization.

As with other systems, it is important to be aware of the corruption risks associated with government in the cyberspace. The first step in building corruption resistance in e-government is identifying the risks and understanding them, some of the risks may be entirely new. These risks need to be identified and understood. Failure by managers to institute controls in Computer Systems due to the myth of computer omnipotence and assumption that ICT removes the opportunities for corruption, is probably the most dangerous tendency. This lack of controls has become evident to those who understand the new technology. It is an opportunity for them to take advantage of the situation.

The guidelines, if implemented, will help the government prevent corrupt practices in computerized organizations and those in the process of computerization. This will ensure there is increased government data security, increased transparency in the implementation of ICT projects and checks in the exercise of discretion by government officials.

Organizational culture can affect both the occurrence, and the perpetuation of, corrupt practices. An organizational culture that ensures procedures are followed counts as a safeguard corruption. Thus it is imperative that the public sector undertakes wide training and sensitization on the move towards e-government and relate such training towards enhancing integrity among the public officers.

LIST OF REFERENCES

1. Information Technology and Public Sector Corruption - ***By Richard Heeks***
2. Transnational Crime, Corruption, and Information Technology – ***By Transnational Crime and Corruption Center***
3. E-government to Combat Corruption **-** ***By Clay G Wescott (Asian Development Bank)***
4. Control Objective for Information and Related Technology (**COBIT)** 4.1 – ***By IT Governance Institute***
5. The Hidden Threat to E-Government – Avoiding large government IT failures – ***By Organization for Economic Co-operation and Development (OECD)***
6. Ethics at work. A guide for business managers in the use of IT – ***By ICAC Hong Kong***
7. The Need to Know eCorruption and unmanaged risk ***– By ICAC New South Wales***