UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING & INFORMATICS

SECURITY IN HEALTH WORKFORCE INFORMATION SYSTEMS: A CASE OF REGULATORY HUMAN RESOURCE INFORMATION SYSTEM

By

MONG'ERI, MARRIANE KEMUNTO

P56/72903/2012

SUPERVISOR

CHRISTOPHER A. MOTURI

A project report submitted in partial fulfillment of the requirement for the Masters of Science in Information Systems of the University of Nairobi

November 2014

DECLARATION

This research project is entirely my original work and where there is work or contribution of others it has been acknowledged. To the best of my knowledge, this research work has not been presented in any other education institution of similar purpose or forum.

Signature: _____ Date: _____

Mong'eri, Marriane Kemunto

Registration Number: P56/72903/2012

This research has been submitted for examination with my approval as the university supervisor.

Signature: _____ Date: _____

Christopher A. Moturi

Deputy Director

School of Computing and informatics

University of Nairobi

ACKNOWLEDGEMENT

I sincerely thank my project supervisor Christopher A. Moturi for his continued patience, guidance and support, and the Project Assessment Panel for their constructive criticism and valuable contribution.

I would like to thank the management of the four Health Regulatory Boards and Councils and their staff who participated in the response to the questionnaires administered: Nursing Council of Kenya (NCK), Clinical Officers' Council (COC), Kenya Medical Laboratory Technicians and Technologists Board (KMLTTB), Medical Practitioners and Dentists Board (MPDB) for allowing me to undertake my research in their institutions.

I am grateful to Emory University Project for giving me their approval to carry out the study and allowing their system and web developers to also take part in response to my inquiries.

My sincere gratitude goes to my family for the love and support during this study. Your being there for me gave me strength to continue amidst the various challenges faced.

Finally, I thank the almighty God who sustained my health and gave me wisdom, strength and courage to complete this work.

ABSTRACT

The health workforce distribution, efficiency and competence are a major concern in health care delivery in Kenya. A well designed health workforce information system can inform policy making to a great extent. However, if health workforce information systems are not well secured, the information can be misleading. The purpose of this study was to assess the level of security in the Regulatory Health Workforce Information System (rHIS) and develop an information security plan for the rHIS. The rHIS is intended to streamline the operations of the Health Regulatory Boards and Councils including routine tracking of training, registration, practice and deployment of the health workforce to make the processes consistent, efficient and effective.

The study assessed the security of rHIS deployment in four regulatory Boards and Councils within the Ministry of Health in Kenya i.e. Nursing Council of Kenya (NCK), Clinical Officers' Council (COC), Kenya Medical Laboratory Technicians and Technologists Board (KMLTTB), Medical Practitioners and Dentists Board (MPDB). The ISO/IEC 27002 standard was adopted as the best practice on information security management. The assessment was based on ISO/IEC 17799:2005 audit checklist. A gap analysis applicability matrix was developed to indicate which questions were asked to which category of respondents in scope.

The results indicated that the system security compliance differed across the Boards and Councils implying that the effectiveness of the security of rHIS is dependent upon the environment on which the system is deployed. It was evident that the compliance level was higher where an information security policy exists.

The study used the gaps identified as a basis to propose a security plan that would provide a way forward in addressing the weaknesses and threats that exists in the various Boards and Councils.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

1.1.Background

1.1.1. Overview

According to the Medical Dictionary, healthcare is the prevention, treatment, and management of illness and the preservation of mental and physical well-being through the services offered by the medical and allied health professions. Healthcare is the diagnosis, treatment, and prevention of disease, illness, injury, and other physical and mental impairments in humans. Healthcare is delivered by practitioners in medicine, chiropractic, dentistry, nursing, pharmacy, allied health, and other care providers. It refers to the work done in providing primary care, secondary care and tertiary care, as well as in public health.

Access to healthcare varies across countries, groups and individuals, largely influenced by social and economic conditions as well as the health policies in place. Countries and jurisdictions have different policies and plans in relation to the personal and population-based health care goals within their societies. Healthcare systems are organizations established to meet the health needs of target populations. Their exact configuration varies from country to country. In some countries and jurisdictions, healthcare planning is distributed among market participants, whereas in others planning is made more centrally among governments or other coordinating bodies. In all cases a well-functioning healthcare system requires a robust financing mechanism; a well-trained and adequately-paid workforce; reliable information on which to base decisions and policies; and well maintained facilities and logistics to deliver quality medicines and technologies (WHO, http://www.who.int/en/).

Kenya is one of the 57 countries globally and one of 36 within sub-Saharan Africa with critical shortages of health workers. For every 1,000 persons in the population, there are fewer than 2.5 health workers, far short of the WHO recommendation for the minimum threshold required for good health care (Crisofari and Hodges, 2011). No health system can function well without an effective and competent workforce.

The Kenya health sector is regulated by seven Boards and Councils, four of which have a functional health workforce information system (www.heath.go.ke). Health regulatory bodies are mandated to regulate the business and practice in specific medical areas like laboratory, nursing, medical practitioners and clinical medicine. The bodies are also expected to advise government in these areas with respect to health workforce.

In Kenya, Center for Disease Control (CDC) worked with Emory University to establish the first Human Resource Information System (HRIS) in sub-Saharan Africa, which collects registration and deployment data on health care workers on a quarterly basis from more than 6,000 health facilities nationwide. The data produced has been used to impact policy and program decisions by the Ministry of Health, such as to successfully extend the retirement age across the whole civil service, including nurses, by five years, and has been replicated across the continent.

Data at the Uganda Nurses and Midwives Council (UNMC) health informatics system has been valuable in monitoring and reviewing information about nurses and midwives. However, information obtained from this system is also important in improving strategic planning for the greater healthcare system in Uganda (McQuide, Matte and Spero, 2011).

The 2011 East, Southern and Central Africa Health Community Forum on best practices passed a resolution by the Health Ministers to support the development of comprehensive human resources information systems (HRIS) at training institutions, regulatory bodies and employers, and to build capacity for HRIS use to inform policy and decision-making (Crisofari and Hodges, 2011).

1.1.2. The Regulatory Boards and Councils

The function of the regulatory Boards and Councils include the following.

Indexing

Every student admitted into a training institution in Kenya to undertake a medical related course must meet preset minimum requirements of admission based on national examinations body (KNEC). Each of the health regulatory Boards and Councils has a unique way of identifying their students. Foreigners who wish to undertake the medical related courses in Kenya are required to have equation of their grades done by KNEC prior to consideration for admission. The process of validating students and assigning of special numbers is termed as *indexing*. The numbers are assigned based on the level of training (certificate, diploma, degree) and the year of admission. The student is thus tracked until the expiration of the expected training period.

Professional Examination

All students who successfully complete training and pass their college qualifying examination are then expected to undertake a professional registration examination. The

examination covers the core areas of training and includes practical testing in some cadres such as medical laboratory profession. Each of the Boards and Councils has designated examination centres and corresponding capacities to ensure quality of examination administration.

Registration

The registration of professionals is dependent on qualifying training and passing the registration examinations. Registration of those trained outside Kenya equally follows the same requirements; however the applicant must provide proof of qualification from the country of training in form of a signed letter of introduction and confirmation. All successful applicants are issued with unique registration numbers and corresponding registration certificates.

Continuous Professional Development (CPD)

Continuous professional development is the in service training that the professionals must undertake in order to keep abreast with recent technologies and other developments in their corresponding professions. The Boards and Councils that have already rolled out CPD have guidelines on what trainings qualify for CPD and the corresponding points to be awarded for each case. The points attained are used as a basis for retention and renewal of professional practicing license.

Licensure

All registered professionals are issued with a practicing license that has to be renewed periodically, annually or after three years for some Boards and Councils, to allow the profession to continue rendering service. The license is issued upon attaining the minimum set CPD points and payments of licensing fees. It is illegal for a professional to practice with an expired license, therefore annually the Registrars and CEOs of these organizations must post in the Kenya gazette the registered and retained professionals by 31st March of every year for public knowledge.

Attrition

Attrition is the process by which personnel leave the profession need tracking. The reasons for leaving the profession are considered to be death, change of profession, outmigration and disciplinary issues leading to suspension or revocation of registration certificates. Not all Boards and Councils have successfully implemented this function.

Training Institution Regulation

The health regulatory bodies have a preset criteria and requirements for any institution that wishes to offer training in medical related courses. The interested party must apply to the relevant body, an inspection is undertaken to ascertain the capacity of the institution to offer the course intended. Upon fulfilling these requirements, the institution is then registered and licensed to offer the course with a fixed number of students depending on the infrastructure. The institution must annually retain their license in order to continue offering the registered courses.

Facility Regulation

Medical related facilities include clinics, hospitals, nursing homes, pharmacies and medical laboratories. The Health regulatory bodies have equally set standards that define the category of the facility based on level of services offered. The standards must be met in order to operate such businesses so as to ensure quality of services delivery. Any interested party therefore must apply for registration with the relevant body, which organizes and undertakes an inspection to ascertain the conditions of operation and infrastructure against the set standards prior to approval of the facility. Any successful facility is issued with a registration number, certificate and license for operation. The licenses must be renewed annually. The certificates and licenses may be revoked in the event of malpractices and poor service delivery.

1.1.3. The Regulatory Health Workforce Information System (RHIS)

Regulatory Health workforce Information System (RHIS) is a modular web-based database system developed by the Emory University project for management and tracking of health professionals. The system modules are mapped onto the existing organization functions which include indexing of students and corresponding internship, professional examination, personnel registration and licensure, continuous professional development, training institutions and facilities inspection, registration and licensure. This system has been implemented in four of the health regulatory bodies with Kenya as the pioneer country in Africa.

System Functionalities

The system functionalities are aligned with the standards and processes defined above. The minimum criteria are preset in the system to minimize human interventions on the system operations. The indexing module, for instance, automatically generates index numbers and

serialized cards for qualified applicants upon meeting the indexing criteria embedded within the system. The rejected applications are equally stored in system for purposes of accountability. The indexing module is then linked to the examination module to allow only eligible applicants to sit for examinations and further generates examination numbers and cards per level of training and examination centres. The system also links the examination module to the registration module to facilitate registration of eligible candidates. The registration numbers are also system generated upon approval by the registration officer who processes the registration applications at system level. The system uses role based approach in management of users. Each officer is allocated roles that are aligned to their job descriptions.

Recent Developments Affecting the RHIS

With the bid to make service delivery more effective and efficient, The health regulatory bodies are introducing online services such as SMS to database querying and online payment. This will necessitate system interoperability among these platforms to facilitate access by various clients. At the same time, Kenya is still dependent upon donor support for funding various programs in the Health sector. This implies that there are numerous activities involving the health workforce that are captured in independent systems. This therefore necessitates that the existing health regulatory human resource information systems have to be opened up for integration to allow seamless exchange of information where necessary. The interoperability of these systems should be clearly defined to cover all dimensions to assure security of the information system.

1.2. Problem Statement

The health workforce distribution, efficiency and competence are a major concern in health care delivery. A well designed information system can provide a reliable reference and basis for decision making and may to a great extent inform policy changes, however if not well secured, any corruption of the information can be misleading. The purpose of this study is to assess level of security in the regulatory health workforce information system (RHIS) and develop a security plan for effective health care delivery.

1.3. Research Objectives

The main aim of the study was to assess the level of Health Workforce Information System security and develop a security plan for effective healthcare delivery. The specific objectives of this study were to:

1. Establish the security controls integrated in the information system of the health regulatory Boards and Councils.
2. Develop a SWOT analysis.
3. Develop a security plan.

1.4. Research Questions

1. Which security controls have been integrated in the information system?
2. What are the strengths, weaknesses, opportunities and threats of the information system security?

1.5. Research Significance

The outcome of this study will be relevant to the following groups:

i. The Kenyan health regulatory bodies that will use the research outcome as a baseline for strengthening their security systems.
ii. Regional health regulatory bodies intending to adopt a similar information system for their health workforce will use the research results for planning purposes.
iii. The ministries of health in the region who may adopt the security plan as a model for their information system.
iv. Researchers of health information systems.

1.7. Justification

Considering the current trends on devolution of services in Kenya, the regulatory bodies are planning to shift their databases to the cloud to facilitate access of services to county level. The Boards and Councils have signed a memorandum of understanding to facilitate data sharing amongst themselves on common areas of operation through the web-based platform. The Boards and Councils are also establishing collaborations with other stakeholders to facilitate system interoperability for efficiency in service delivery such as online payment and SMS database querying to allow access of service on anytime anywhere basis. With the rise in cybercrimes there is need for integration of high levels of security to safeguard the information against loss of integrity, confidentiality and availability.

1.8. Scope of Study

The study was carried out in four health regulatory bodies namely:

i. Kenya Medical Laboratory Technicians and Technology Board (KMLTTB)
ii. Nursing Council of Kenya (NCK)
iii. Clinical Officers Council (COC)
iv. Medical Practitioners and Dentists Board (MPDB)

1.9. Assumptions and Limitations

This study made the following assumptions:

i. All health regulatory bodies have functional information systems
ii. Guaranteed willingness of respondents to participate in research

This study was limited by the following factors:

i. There may be no means to audit system configurations.
ii. Information system security is wide and it might not be possible to asses all aspects.

CHAPTER TWO: LITERATURE REVIEW

2.1. Health Workforce

The main intention of the Health surveillance and informatics systems in the health regulatory Boards and Councils is to assist in routinely tracking the training, registration, practice and deployment of the health workforce. The data from these systems should help Ministries of Health make evidence-based decisions on strengthening the health workforce.

A report from Centre for Disease Control (CDC, http://www.cdc.gov/) on building a sustainable health workforce indicates that effective public health systems depend on a trained and motivated workforce to carry out the services needed to achieve health goals however it is further noted that establishing sustainable public health workforce capacity is more than just training—it requires strengthening a complex system of human resource dynamics, including: planning and management of the health workforce; producing new health workers through pre-service education; ensuring adequate recruitment into the public health system; improving the quality of training, mentorship and supervision; and providing appropriate retention incentives.

According to the Kenya Vision 2030 (http://www.vision2030.go.ke/) economic pillar that seeks to improve the prosperity of all regions of the country one of the six priority sectors is IT enabled services. The social pillar on the other hand has an objective of investing in the people of Kenya in order to improve the quality of life for all Kenyans by targeting a cross-section of human and social welfare projects and programmes. Health is one of the specific areas of concern under this pillar.

The second annual report on implementation of first medium term plan (2008-2012) of Kenya vision 2030, notes that the ICT sector is significant in providing essential services required for Kenya's social, economic and political development (http://www.vision2030.go.ke). Sound and responsive policies, legal and institutional frameworks are, however, necessary for the sector to realize its full potential. The report further highlights that an ICT policy has been developed, an e-government strategy paper developed and launched in order to provide a roadmap for the delivery of improved and efficient services to the public. Measures are also underway to establish the infrastructure required to facilitate delivery of online government services to the public which is to be undertaken at the county and constituency levels. Some of the institutional reforms that have been undertaken include establishment of a government data centre to facilitate the storage of

all government databases. All ministries, departments and agencies have been requested to provide content for the Government Data Center.

The report also indicates that the efficacy of ICT has not been fully exploited with a main constrain being that of poor and inadequate ICT infrastructure in the country. Among the many challenges are weak institutional and legal frameworks, particularly to govern automated services and electronic transactions. In order to provide efficient service, The Health regulatory bodies will have to embrace online payment technology and equally consider cloud services for hosting of their various database management systems to enable interaction with their clients through their websites (ME, 2011)

2.2. Interoperability Concept

Interoperability is defined as the ability of disparate and diverse organizations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organizations via the business processes they support, by means of the exchange of data between their respective ICT (EIF, 2004)

Interoperability has three main dimensions.First is the technical interoperability dimension which covers the technical issues of linking computer systems and services. It includes aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility, and security services. Second is semantic interoperability dimension that is concerned with ensuring that the precise meaning of exchanged information among computer systems and services is understandable, even though they were not initially developed with the purpose to interoperate. Semantic interoperability enables systems to combine received information with other information resources and to process it in a meaningful manner. Finally the organizational interoperability dimension which is concerned with defining business goals, modeling business processes, and bringing about the collaboration of administrations that wish to exchange information and may have different internal structures and processes. Moreover, organizational interoperability aims at addressing the requirements of the user community by making services available, easily identifiable, accessible, and user oriented (Soares and Amaral, 2011)

2.3. Information Security Controls and Perceptions

Information is considered secure when measures have been put in place to mitigate loss of confidentiality, integrity and availability of that information. Confidentiality preserves

authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Integrity guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity whereas availability ensures timely and reliable access to and use of information. (Swanson et al, 2010)

Critical elements of any useful information security program are risk analysis and risk management. Where the security analysis reveals the organization's value for information and its risk of exposure and the risk management is done within a security framework encompassing administrative, personnel and physical controls.

2.3.1. Information Security Controls

Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept.

Physical security is the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from espionage, theft, and destruction or damage by accident, fire, or natural disaster. Technical security control on the other hand involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices which include access control software, antivirus software, library control systems, passwords, smart cards, encryption, dial-up access control and callback systems. Administrative, or personnel, security consists of management constraints, operational procedures, accountability procedures, and supplemental administrative controls established to provide an acceptable level of protection for computing resources. In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances such as security awareness and technical training, separation of duties, procedures for recruiting and terminating employees, security policies and

procedures, supervision, disaster recovery, contingency and emergency plans and user registration for computer access (Krause and Tipton).

2.3.2. Information Security Perceptions

a) Information security management and operation

Security management and operations effectiveness and efficiency varies widely across enterprise organizations. There are dimensions that tend to characterize security best practices and commitment namely perception of security whether information security is aligned to organization corporate culture or integrated into specific business processes, whether the CISO is perceived as a business or IT executive, whether executive management is fully or partially engaged in strategy and situational awareness and whether the organization has a security incident and event management deployed or is planning to adopt the same. Strong information security depends upon an integrated mix that includes organizational leadership, formal policies, documented processes, skilled tacticians, and layers of complementary technical defenses addressing specific aspects of security management and operations such as risk management, incident detection, and incident response (Oltsik, Kao and Gahm, 2012).

There are three specific aspects of security management and operations: risk management, incident detection, and incident response. Strong information security depends upon an integrated mix that includes organizational leadership, formal policies, documented processes, skilled tacticians, and layers of complementary technical defenses. Change in Information security management and operations is driven by technologies such as server virtualization, cloud computing, web-based applications, and mobile devices. Information security strategy in most organizations is driven by two primary motivations: protecting sensitive data / intellectual property and regulatory compliance (Oltsik, Kao and Gahm, 2012).

b) User role in information system security

A review of user role in information security indicates that no technical solution can make an information system more secure than the processes of the people who use it. Poor user practices can compromise the best security systems implemented in any system. Compliance base solutions do not necessarily equal effective security. Organizations that have a security standard to comply with often measure success as a function of technical implementation of compliance controls leading to a misunderstanding of the importance of other aspects such as

managerial policies and operational procedures. Information security thinking is often server and desktop focused, giving virtually no attention to protecting the mobile and portable technologies many workers use most.

The review further indicates that users also suffer from a lack of clarity about information security. Many organizations do an inadequate job of defining and implementing good policies, counting instead on compliance measures, technical mechanisms or a thinly staffed, overworked (and sometimes even non-existent) security team to protect them. Even those organizations that have thought through their information security policies often do a poor job of communicating them to users. Many security systems are entirely undocumented. Others are presented as unexplained mandates, which users find easy to dismiss as mere roadblocks to their productivity or, more negatively, as territorial directives from an IT group that is out of touch with their routine work needs. An informal framework without meaningful and clearly documented procedures can be just as bad as relying exclusively on mandates – it creates the perception that information security is optional and encourages the prioritization of workflow over security. A lack of clear management support can also create a casual attitude that favors workflow over data protection. If senior members of the organization do not prioritize security, users often cannot. Any effort to protect information must be supported by adequate specialist staffing, adequate resources and ongoing education at all levels or it risks failure (Motorola, 2010).

2.4. Risk Management

The process of risk assessment is pivotal in an organizations information security. A risk assessment allows an organization to determine how and where to spend its money in its efforts to protect itself. Generally the outcome of a risk assessment is a prioritized list outlining what business processes are at the most risk, what the risks are and what controls can be implemented to deal with the risk. Although risk assessments are not unique to the IT field, they do provide a unique application of the process (Skyler, 2011).

2.5. Seven Stages of Advanced Threats

Advanced threats are targeted towards information and intellectual property contained in organization databases as opposed to traditional threats that targeted the systems.They utilize tactics such as social engineering,exploiting software vulnerabilities and blind spots embedded in the traditional security setups.There are instances where security approaches focus on the web servers and forget about the end users who are the main target of advanced

attackers.There are seven distinct stages of advanced threats as shoen in Fig 1 (Clark and Robinson, 2013):

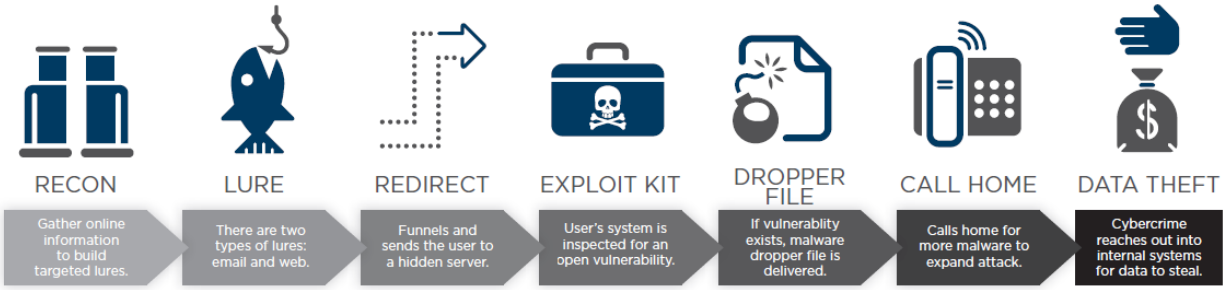


Figure 1: Stages of Advanced Threats

i. Reconnaisance, lure and redirect- information gathering for the hacker to position themselves for compromise of an adversary or someone else.where the hacker establishes the organization's area of interest and creates activities of interest to capture the users attention and invite them to participate.

ii. Exploit and dropper file-change of mode of operation,previously security personnel would share out vulnerabilities to help put up relevant counter measures but currently people search for the threats to be able to exploit the weaknesses.

iii. Call homes and data theft- most organizations use SSL for secure transmission of data to secure the organizationa dn also protect end users,however the hackers are using the same tactic for exfiltration of data over secure channels that leave them unidentified.Data theft also takes place through simple things as screenshots and at times when the user is off their organization's protected network and is least aware of the network security.

2.6. Security Approaches, Frameworks and Standards

Most organizations are ill prepared on defense towards advanced attacks because they do not understand what they are trying to protect. They assume it could be the data, the intellectual property, the information but do not even know where that sits. Organizations further invest in passive security solutions that only detect attacks yet they are supposed to focus on detecting maintaining and mitigating the attack. In security the focus should be on confidentiality, integrity and availability but most organizations invest in infrastructure security instead of data centric security (Clark and Thacker, 2013). There exists a number of internationally recognized standards and frameworks that guide information security namely: ISO/IEC 27002, COBIT, ISACA, ITIL and NIST.

2.6.1. ISO 27002

ISO 27002 defines information security as the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met and this should be done in conjunction with other business management processes (JTC, 2007).

The standard covers the following twelve core areas:-

1. **Risk management** which entails determining asset vulnerability. The organization should undertake risk assessment, analysis and mitigation.
2. **Security Policy** that provides the management direction through documented principles, policies, standards, guidelines and procedures.
3. **Organization of Information Security** - governance of information security. An elaborate structure and reporting mechanism including liason with the relevant offices.
4. **Asset Management** that deals with inventory, classification and ownership of information assets.
5. **Human Resources Security** detailing the security aspects for employees joining, moving and leaving an organization including awareness training and education of these employees.
6. **Physical and Environmental Security** that involves protection of the computer facilities in terms of physical access, air conditioning, fire and water.
7. **Communications and Operations Management** detailing management of technical security controls such as archives, backups, logging, patching, monitoring and configurations.
8. **Access Control** that entails restriction of access rights to networks, systems, applications, functions and data
9. **Information Systems Acquisition, development and maintenance** that emphasizes on building security into applications by following the proper system development life cycle
10. **Information Security Incident Management** by anticipating and responding appropriately to security breaches.

11. **Business Continuity Management** covering protection, maintainance and recovery of business-critical processes and systems.
12. **Compliance** - ensuring conformance with information security policies, standards, laws and regulations

2.6.2. COBIT

Control Objectives for Information and related Technology (COBIT) provides guidance on IT governance. IT Governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives (ITGI, 2007). The following core areas are covered by COBIT

i. **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
ii. **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
iii. **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.
iv. **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organization.
v. **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

2.6.3. ITIL

The IT Infrastructure Library (ITIL) provides a framework of Best Practice guidance for IT Service Management. A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. Therefore service management is a set of specialized organizational capabilities for providing value to customers in the form of services. Each service, process or infrastructure component

has a lifecycle, and service management considers the entire lifecycle from strategy through design and transition to operation and continual improvement which ensures that the IT services are aligned to the business needs and actively support them (Cartlidge et al, 2007). ITIL focuses on the following areas:

i. **Service Strategy**: shows how to transform service management into a strategic asset.
ii. **Service Design**: guidance on designing IT services, along with the governing IT practices, processes and policies, to realize the strategy and facilitate the introduction of services into the live environment ensuring quality service delivery, customer satisfaction and cost-effective service provision.
iii. **Service Transition**: guidance for the development of capabilities for transitioning new and changed services into operations, ensuring the requirements of Service Strategy, encoded in Service Design, are effectively realized in Service Operations while controlling the risks of failure and disruption.
iv. **Service Operation**: guidance on achieving effectiveness and efficiency in the delivery and support of services to ensure value for the customer and the service provider. Strategic objectives are ultimately realized through Service Operations.
v. **Continual Service Improvement**: guidance in creating and maintaining value for customers through better design, introduction and operation of services, linking improvement efforts and outcomes with Service Strategy, Design, Transition and Operation.

2.6.4. NIST

National Institute of standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets. One of the documents developed by this body is Contingency Planning Guide for Federal Information Systems. It indicates that effective contingency planning includes incorporating security controls early in the development of an information system, and maintaining these controls on an ongoing basis. (Swanson et al, 2010). It provides a seven step contingency planning process as follows:

i. **Develop the contingency planning policy statement.** A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
ii. **Conduct the business impact analysis (BIA).** The BIA helps identify and prioritize information systems and components critical to supporting the organization's

mission/business processes. A template for developing the BIA is provided to assist the user.

iii. **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

iv. **Create contingency strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

v. **Develop an information system contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

vi. **Ensure plan testing, training, and exercises.** Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

vii. **Ensure plan maintenance**. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

2.7. Framework Adopted

This study adopted the ISO/IEC 27002 standard as the best practice on information security management. The ISO/IEC 17799:2005 audit checklist was used as the assesment tool. Several prveious work was taken into consideration in adopting this frameowrk.

Wiander (2007) analyzed the implementation experiences of some organisations that have implemented the ISO/IEC 17799 standard and their results suggests that the standard served the needs of the small and medium-sized enterprises well and its intended usage correlates well with the practices of such organizations.

Boehmer (2008) demonstrates the use used ISO27001 as a method for measuring the performance of the implementation and operation of an information security management system.

Gillies (2011) considered the global adoption of the ISO27000 series of standard, and compared them with the adoption rates for ISO9000 and ISO14000. They provide a step-by-step framework designed to simplify the process for organisations working towards ISO27001 and offer significant benefits at milestones before systems are mature enough to achieve certification.

Liao and Chueh (2012) assessed the level of attention provided to information security management by medical personnel in Taiwan and developed an evaluation framework based on the ISO27001 standard for information security management.

Lindström and Hägerfors (2009) proposed a model that can be used to explain strategic IT and information security as well as for training purposes with regards to senior management. This is because of the importance of senior management ownership and care for strategic elements of the organization's security programme.

Tashi and Ghernaouti-Hallie (2007) discussed the reasons for having a well defined managerial security framework by analyzing advantages and limitations of the ISO 17799 and ISO 27001 standards and the implications of conformity to the standards.

CHAPTER THREE: METHODOLOGY

3.1 Research Design

This study utilized both qualitative and quantitative techniques. Qualitative research techniques are exploratory, and used when we don't know what to expect, to define the problem or develop an approach to the problem. It is also used to go deeper into issues of interest and explore nuances related to the problem at hand. Qualitative methods include reviews, interviews and observations. Quantitative research techniques are those that produce hard numbers which can be turned into statistics. Such methods include surveys and audits with questions that have Yes or No answers that can be categorized and quantified. Both methods in this study attempted to accumulate existing information and data regarding the information system security levels to depict the current state.

3.2 Sources of data

The main sources of data were the interactions and interviews with registrars and chief executive officers, end users, ICT personnel in the four health regulatory boards and councils: Nursing Council of Kenya (NCK), Clinical Officers' Council (COC), Kenya Medical Laboratory Technicians and Technologists Board (KMLTTB), Medical Practitioners and Dentists Board (MPDB). Data was also gathered from organization documents such as policies, guidelines, business process documents and standard operating procedures.

3.3 Sample Design

The research involved a sample of 38 personnel being the system users in the various Boards and Councils: Four (4) IT personnel, Two (2) system developers, Four (4) top managers (registrars/CEO), Thirty (28) end users (see appendix III for details):

3.4 Tools Procedures and Methods of Data Collection

The content of the data collection tools was developed based on the ISO IEC 17799:2005 information security audit checklist. The standard provides a list of audit areas, that according to ISO27000 forum of 2011, the interested party can develop a gap analysis applicability matrix defining how each of the questions will be handled. The research therefore categorized the questions into six main areas namely: document review, observation, developers, end users, management and IT personnel (see appendix VI).

Structured Questionnaires

Structured questionnaires covering specific aspects of security were administered to end users including heads of departments to facilitate gathering of information on the current state of the organization information security. This tool was given preference over the others as there were 30 end users (Heads of departments and other staff within the departments) to be interviewed, the tool would therefore provide a standard format of questions for all respondents making the process simpler and consistent and further provide comfort for the respondents who may shy away from interviews for fear of their management. The only disadvantage of this approach is that not all aspects of security could be captured in a questionnaire. However this was be addressed through the other tools to be used in this study.

Structured Interviews

Structured interviews were undertaken by the registrars and CEOs of the organizations, summing to a total of four personnel. This mode of data collection was considered appropriate for this group as the number was small and the information required was not too detailed to capture in a questionnaire. The structure also ensured that the data collected was consistent and uniform across all the four health regulatory boards and councils.

Document Review

The existing IT policies and business process operation documents were reviewed against the areas identified in the applicability matrix.

Observation

Site visits were conducted during which observations were made and documented. This assisted in collecting of information that the organization would not willfully give concerning their information security status.

3.5 Data Analysis

The findings were recorded back into the gap analysis matrix. Microsoft Excel pivot tables were used in the analysis of the data collected.

A daily interpretative analysis (DIA) of the interviews undertaken was done at the end of each interview. This entailed review of notes taken and filling of the gap analysis matrix based on interpretation of the information obtained. This method was preferred as there are insights that one gets when they listen to a respondent that may seem self-evident at the time, and may appear to be something that cannot be forgotten however such insights turn out to be very hard to remember and as time passes, they lose a great deal of detail and nuance.

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1. Security Controls

The investigations undertaken were guided by ISO 17799:2005 audit checklist. The following key areas were covered:

i. Information security policy
ii. Organization of information security
iii. Asset management
iv. Human resources security
v. Physical and environmental security
vi. Communications and operations management
vii. Access control
viii. Information system acquisition, development and maintenance
ix. Information security incident management
x. Business continuity management

From the investigations undertaken, it was noted that the approaches to security are majorly physical and administrative. The following are the findings based on the ten areas mentioned above:

Table 1: Summary of Scores per Area of Audit

	KMLTTB	**NCK**	**COC**	**MPDB**	**TOTAL**	**KMLTTB2**	**NCK2**	**COC2**	**MPDB2**
Area of audit						**%**	**%**	**%**	**%**
Security Policy	4	7	0	0	10	40	70	0	0
Organization of IS Security	4	7	3	7	9	44	78	33	78
Asset Management	5	5	1	3	7	71	71	14	43
Human Resource Security	6	14	5	7	17	35	82	29	41
Physical and Environmental Security	11	13	8	12	21	52	62	38	57
Communications and Operation Management	29	33	18	23	55	53	60	33	42
Access Control	26	27	12	16	40	65	68	30	40
IS Acquisition, Development and Maintenance	21	24	16	17	33	64	73	48	52
IS Security Incident Management	7	12	0	0	13	54	92	0	0
Business Continuity Management	0	3	0	3	10	0	30	0	30

It is evident that all the organizations had a serious challenge in meeting the security standards across multiple categories, which demonstrates lack of good security practices and in turn puts the information system at risk.

4.1.1 Security Policy

Security policy covered areas such as the existence of the security policy document, its approval, publishing and communication to the users. There was a further check on management commitment and whether the organization's approach to managing information is clearly stated with a procedure for review.

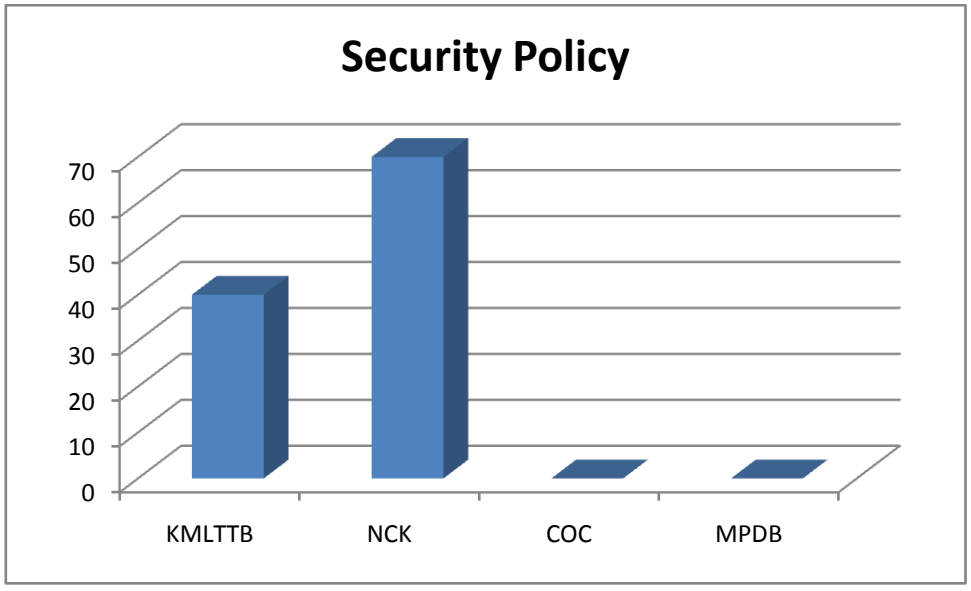


Figure 2: Level of compliance in security policy

It was noted that KMLTTB and NCK have elaborate IT policies however only NCK's policy has been approved by management, published and communicated to some of the employees. The policies state management commitment but only in NCK was the management involved in the development of the policy and is aware of the content and has played a major role in ensuring its implementation. In both cases the policies have never been reviewed, however the policy statement on development allows for periodic reviews to reflect changes in organization operations.

4.1.2 Organization of Information Security

The organization of information security addressed internal and external organization of information security to establish management commitment to information security, the diversity of representatives involved in coordination of security activities and their corresponding roles, clarity of definition of non disclosure agreements, whether risks

associated with external parties have been identified, necessary security action taken such agreements with third parties prior to granting access.

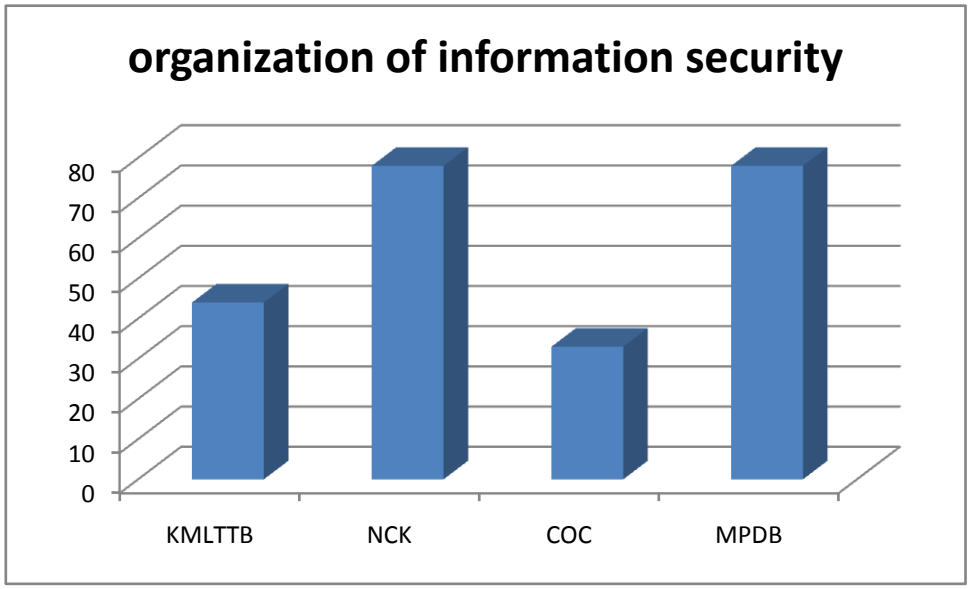


Figure 3: Level of compliance in organization of information security

In internal organization, there was an indication of management commitment to supporting security activities in all the regulatory bodies. In NCK the management was committed to ensuring non-disclosure agreements are signed prior to start of employment of any new personnel. However in terms of information security coordination it was realized that in KMLTTB, COC and MPDB it was considered an IT function instead of having representation from diverse departments of the organization with pertinent roles and responsibilities. In terms of external parties, there has been no risk identification done relating to external parties however measures have been undertaken to only allow authorized access to facilities in all the four bodies.

4.1.3 Asset Management

In Asset management the study covered responsibility for assets and information classification. There is a demonstration of responsibility for assets in all the bodies where there is existence of an assets inventory with clear definitions of owners and acceptable use of assets associated with information processing. However in COC the equipment ownership is not defined.

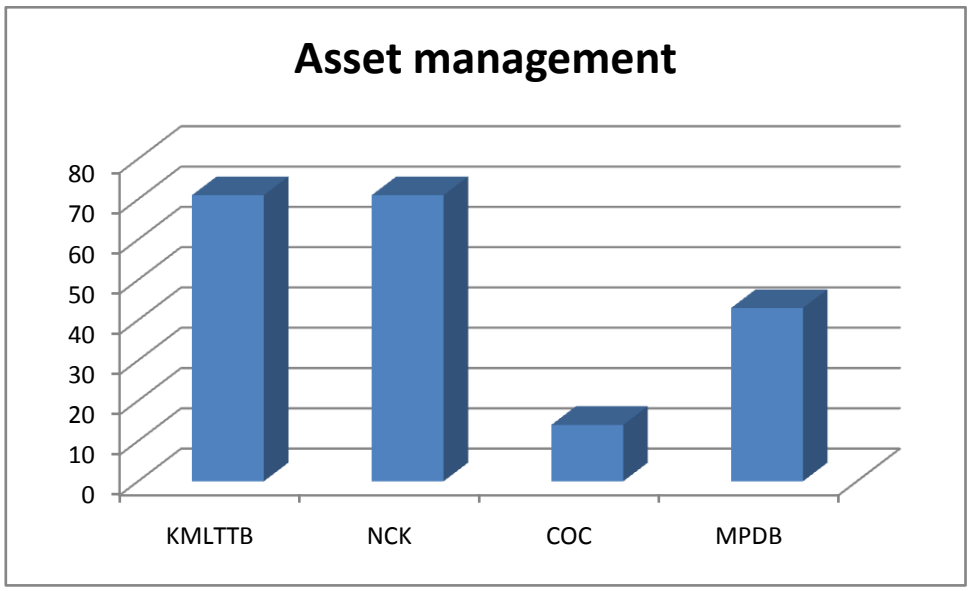


Figure 4: Compliance in asset management

As pertains to information classification, only NCK & KMLTTB have policy statements on information categorization that further states that it is the responsibility of the user to categorize the information they process. However most users have not developed procedures on classifying the information they deal with and have thus not categorized the same.

4.1.4 Human Resources Security

Human resource security undertook consideration of procedures followed prior to, during and termination or change of employment for the organizations' employees.

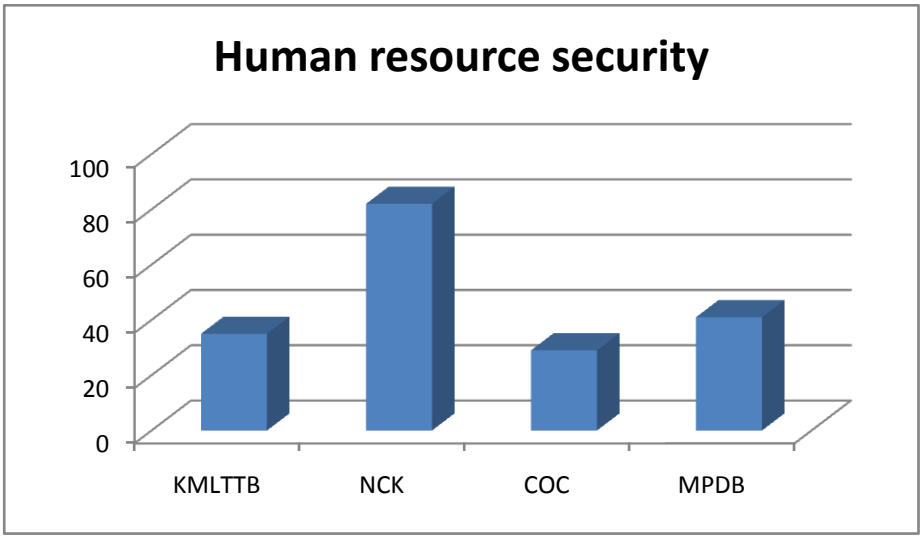


Figure 5: compliance in human resource security

It was noted that only NCK has defined security roles and responsibilities for their employees and undertakes screening and ensures that confidentiality agreements are signed prior to

employment and engagement of a third party. During employment, the IT policy further clearly states disciplinary measures for any security breach. Most of the users in all the bodies confirmed not having received any security awareness training in the recent past. The existing equipment inventory forms have provision for return of assets and signing for the same, the IT policy is also clear on the procedure for removal of access rights. However only NCK and KMLTTB have an IT policy, COC and MPDB have no documented procedure on revocation of access rights.

4.1.5 Physical and environmental security

This section investigated secure areas and equipment security.

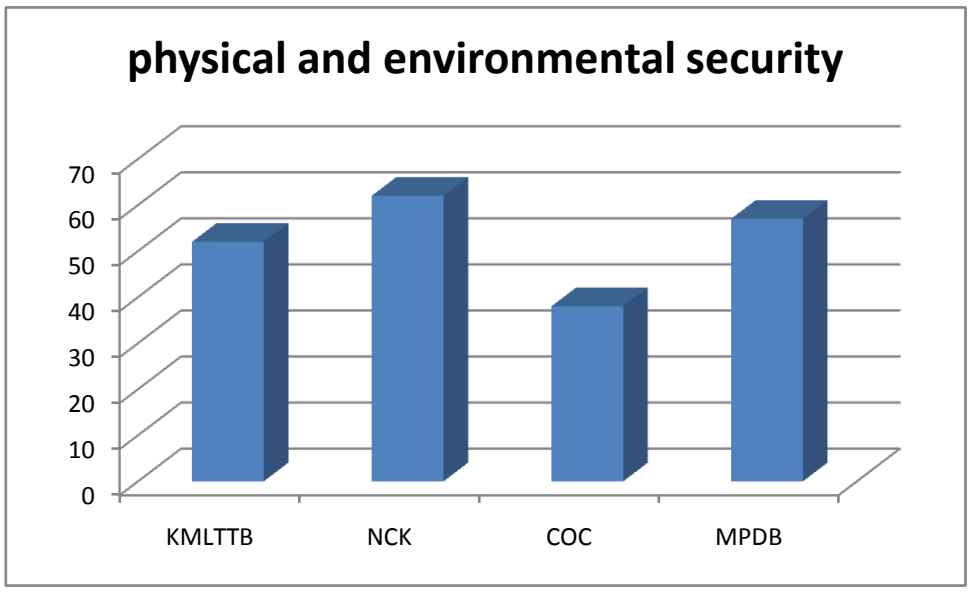


Figure 6: Level of compliance in physical and environmental security

Physical and environmental security has been implemented in different ways to ensure secure areas. In all bodies there are manned receptions, in NCK and KMLTTB there are locked server rooms whereas in COC and MPDB the servers reside in the IT offices that are not well secured. Protection from environmental threats such as floods and fire is not addressed and identification of potential threats from neighboring premises have not been identified.

In regard to equipment security, from observation it is evident that most Central Processing Units (CPUs) sit on the desktops and others directly on the floor. However in all the regulatory bodies there are Uninterruptible Power Supplies to guard against power failures. The network and power cables are also well secured in trunks to avoid interception and damage.

Equipment maintenance is undertaken internally by the IT personnel in all cases as per their maintenance schedule but not according to the suppliers' recommended service intervals as in most cases the IT personnel confirmed only giving special attention to equipment when they breakdown and cease to operate as expected. Any maintenance to be undertaken by an external party is done within the organizations premise; none of the bodies sends their equipment off premises.

To assure secure disposal or re-use of equipment, the NCK and KMLTTB IT policies state that the media should be reliably erased or physically destroyed prior to disposal.
The removal of equipment from the premises is authorized and a gate pass issued in all cases.

4.1.6 Communications and Operations Management

This section was based on operational procedures and responsibilities, third party service delivery management, system planning and acceptance, protection against malicious and mobile code, backups, network security management, media handling, exchange of information, electronic commerce services and monitoring.

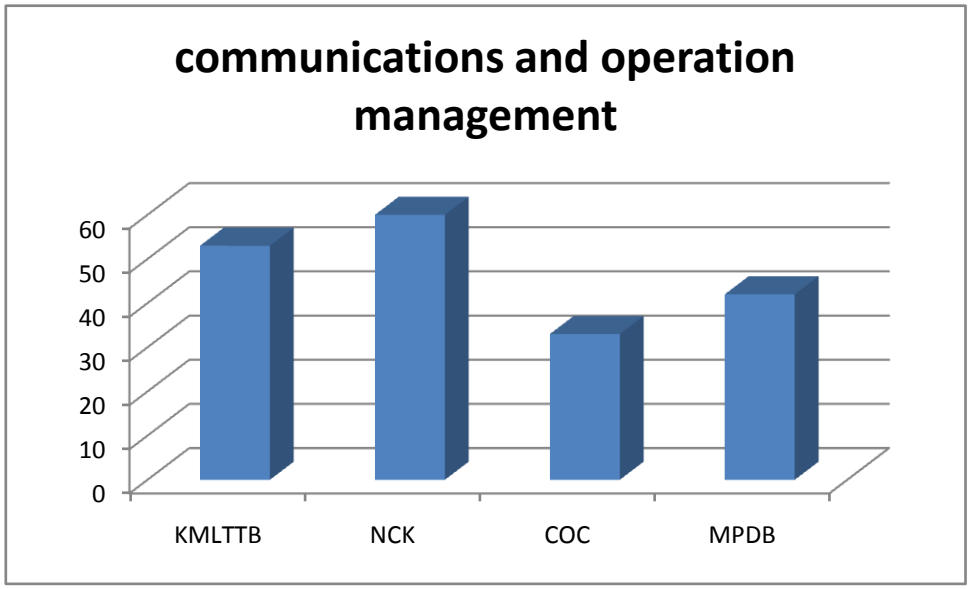


Figure 7: Level of compliance in communications and operations management

It was noted that all the regulatory bodies were in the process of documenting and finalizing their standard operating procedures. This is ongoing with the support of Emory University project, the template in use makes provision for ownership, approval, circulation and review logs.

Change management is covered in the NCK and KMLTTB IT policies and there is a corresponding change request form that captures the relevant fields however this form is only implemented in NCK.

NCK and MPDB have documented job descriptions detailing the duties and areas of responsibilities. There is provision for segregation of duties within the system however this is implemented partly based on documented job descriptions, where they exist, and through logical process understanding by the administrators in the absence of job descriptions.
Development and operational facilities are distinctly isolated in all the bodies. Any new software or modification is first tested from the developer's machine prior to running it on the operational facility.

Third party service delivery is controlled by third party agreements embedded in the IT policies. However this is only implemented in NCK. KMLTTB relies on contracts signed during procurement of services, which does not capture the technical aspects. COC and MPDB do not have a clear way of handling the third parties. NCK,COC and MPDB undertake system planning by monitoring capacity demands and projecting future requirements. The three also have system acceptance criteria for new information systems, upgrades and new versions. None of the bodies have mobile access to their systems. There is use of firewalls in all cases as a control against malicious code.

Backups are done on external hard disks that reside within the organizations, however none of the bodies undertakes testing of the backups to confirm whether data can be recovered in case of a disaster of media failure.

The network management is done internally by the It personnel.This is achieved through use of server based domain control. On the other hand handling of exchange of information is documented in the Data sharing Memorandum of Understanding between Boards and Councils. There is no definite information exchange agreement and electronic commerce services guideline in all the four bodies. However the online transactions map onto the existing local processes.
The regulatory Human Resource Information System (rHRIS) has audit logs that monitor user activities. These are only accessible by the system administrator. However from observation, the system clocks of individual user machines are not synchronized.

4.1.7 Access Control

The areas considered here were business requirement for access control, user access management, user responsibilities, network access control, operating system access control, application and information access control, mobile computing and teleworking.

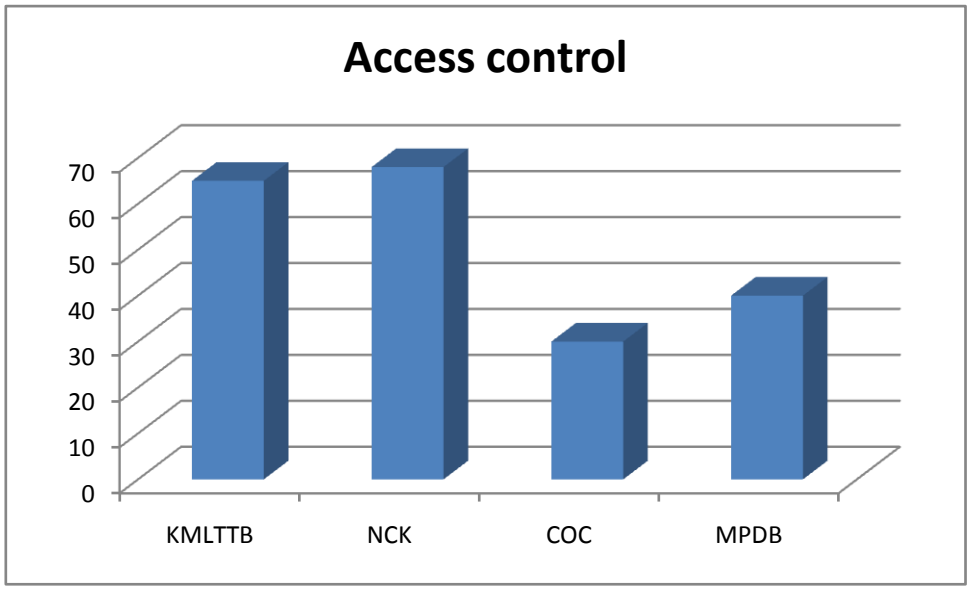


Figure 8: Compliance levels in access control

There exists an access control policy in KMLTTB and NCK. All the system users in the four bodies undergo authentication by use of controlled passwords. None of the bodies have a policy on periodic review of user access rights.

In terms of user responsibility, most users claimed they are not guided on how to select passwords. They further indicated that they do not know how to handle unattended user equipment.

Network access is defined in the existing policies but only implemented in NCK. Mobile computing is also covered in the policies which cover the risks of working with mobile devices and the best practices in their use. COC and MPDB that have no policies do not have guidelines on mobile computing.

4.1.8 Information Systems Acquisition, Development and Maintenance

This section covered security requirements for information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support processes, technical vulnerability management.

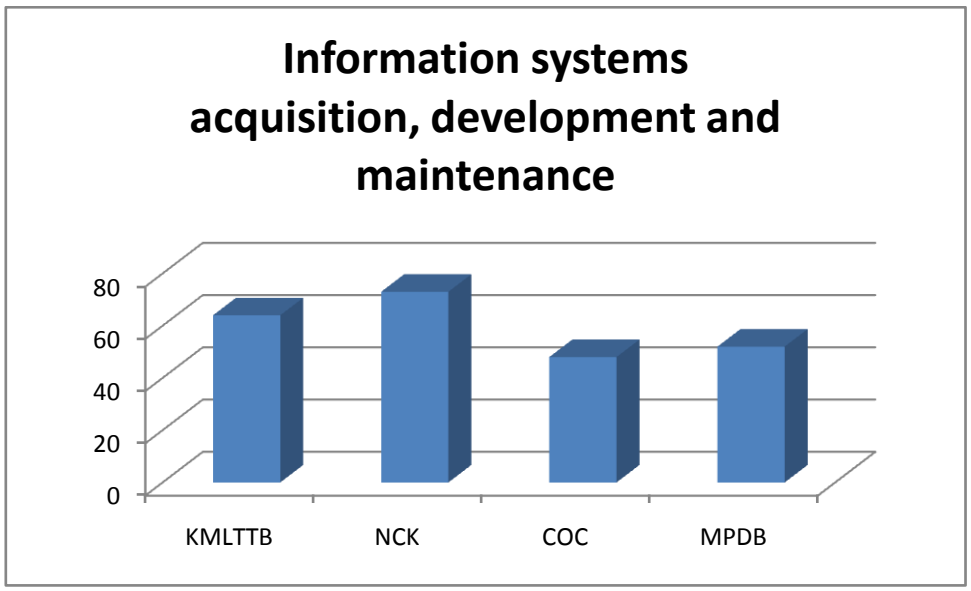


Figure 9: Compliance level in systems acquisition, development and maintenance

It was noted that the developers undertook security requirements of the system prior to implementation based on the environment on which the system was to run. The data validation checks are also taken care of by ensuring that the fields in the various forms are correctly captured, further to this, fields with dates have inbuilt calendars and date differences are auto calculated by the system e.g. time difference between student admission and professional registration. Error handling module has only been implemented in one of the bodies, the rest have to undertake error checking manually.

Data output is also validated through use of system inbuilt reports for all modules to ensure correct and appropriate processing of stored information.

There is no use of cryptographic controls in any of the bodies. Access to system files is restricted to the developers and system administrators. However no technical vulnerability evaluation has been undertaken to inform appropriate measures in mitigating the associated risks.

4.1.9 Information Security Incident Management

The areas covered in this section were reporting information security events & weaknesses and management of information security incidents and improvements

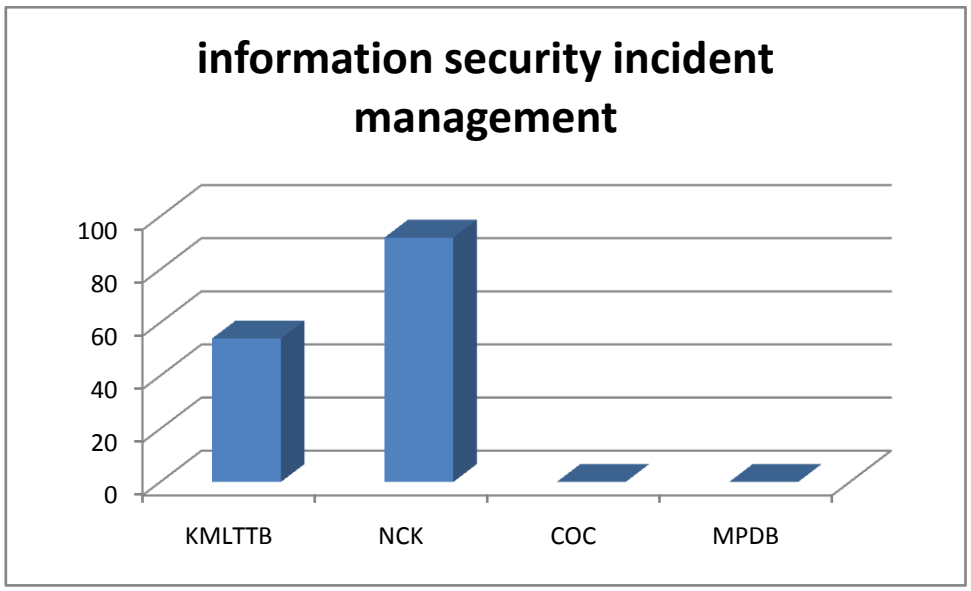


Figure 10: Level of compliance in information security incident management

In one of the bodies, some users confirmed that they have occasionally reported incidents but the modes of reporting differed indicating lack of consistency in reporting procedure. However the IT policies define the process of incident reporting and the corresponding responsible team that handles the reports. The other bodies did not have documentation of security incidences though they have had some security related problems.

4.1.10 Business Continuity Management

It was noted that only NCK and MPDB have business continuity plans. Lack of business continuity plans in COC and KMLTTB poses a great security risk in case of any disaster as the organization may not be prepared to mitigate the risk.

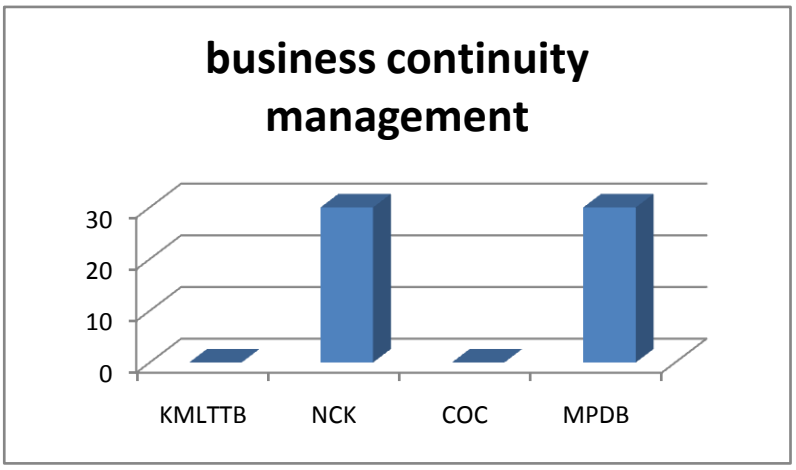


Figure 11: level of compliance in business continuity management

4.2. Discussion

The ISO 27002 standard provides guidance on how an organization should approach information security. The starting point is an organization information security policy whose main objective is to provide direction on security governance and implementation. The analysis as indicated on figure 2 indicates that only half of the organizations had security policies. It was evident that where there is an information security policy, the organization demonstrated a higher level of compliance to recommended standards as opposed to where there was lack of a policy. This is demonstrated in table 1 where NCK scored higher than 60% compliance in all of the 12 areas that were assessed. This implies that the Boards/Councils require an Information security policy in order to take a strategic approach in management of security as lack of policy will lead to ad hoc approach.

Findings on asset management, section 4.1.3, indicate that users have not classified the information that they process. Analysis on human resource security in section 4.1.4 indicates that more than half of the Boards and Councils scored less than 40% as there are no proper screening of employees and contractors, neither do employees have defined roles and responsibilities. This indicates that the system is under great risk as its users are not profiled and may be utilizing the system in an unacceptable manner. According to California office of information security program guide for state agencies (CISPP 2008),because of their internal access levels, authorized users pose a potential threat to systems and data hence there is need to undertake measures to ensure employees and contractors authorized to access or maintain systems have appropriate levels of access needed to perform their duties.

Figures 9, 10& 11 indicate that the Boards and Councils do not have effective controls in place for information systems acquisition, development & maintenance, information security incident and business continuity management. No risk assessment in relation to their internal and external environment has been done. This implies that these organizations will not be able to detect and respond to incidents that threaten the availability of their environments, indicating that their systems are vulnerable to both unauthorized access and downtime. There is also a likelihood that the Boards and Councils will waste resources on areas of minimal risk while leaving the critical areas exposed.

4.3. System Vulnerability

The system vulnerability to attacks can be taken to be an inverse of the compliance to the aspects covered by the audit checklist, based on the discussion above. The system of the

organization that was found to be compliant is considered to be less vulnerable as compared to that of the non-compliant organization. Below is the general graphical representation of compliance:

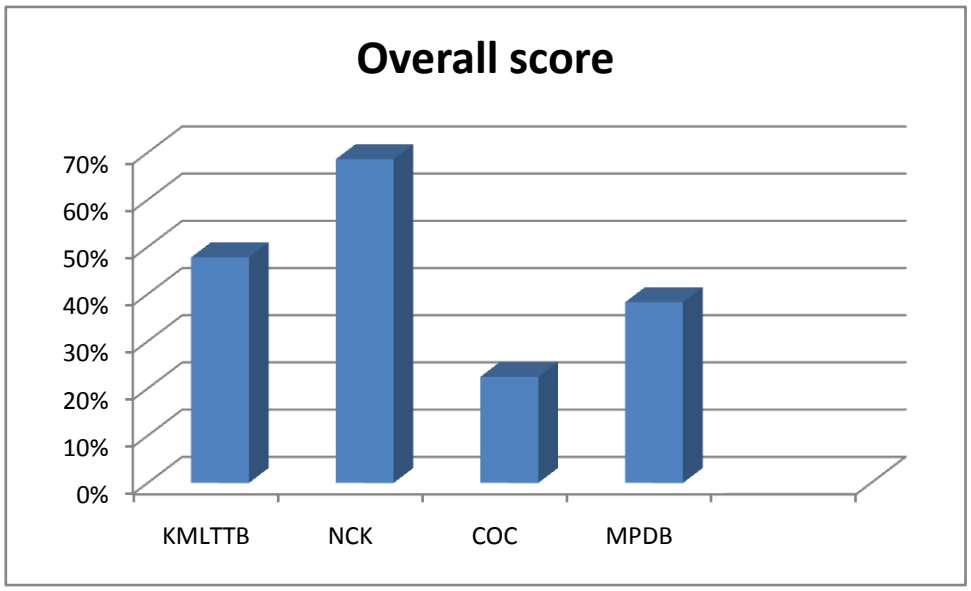


Figure 12: Overall compliance per organization

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5.1. Achievements

The study successfully Implemented the ISO 27002 standard and ISO IEC 17799:2005 checklist in realization of its objectives.

The first objective of the study was to establish the existing security controls. Results indicate that different security elements have been implemented and that the Boards and Councils rate differently in terms of compliance to the recommended security best practices.

The second objective was to assess the vulnerability of the system. This was done based on the levels of compliance attained by each Board and Council. Where the results clearly showed that the system of the highly compliant Board/Council is less vulnerable as compared to that of the less compliant.

The final objective was to propose a security plan that best suits the Boards and Councils. The proposed security plan (Appendix I) is based on the gaps identified across all the four Boards and Councils. The plan offers a step by step approach on how to realize the security best practice in the areas covered by the ISO 27002 standard.

5.2. Limitations of the Study

The study did not take to consideration a vulnerability self assessment of the various Boards and Councils. This would have been important to affirm to the analysis based on compliance.
The study assumed that the proposed security plan can be implemented across all Boards and Councils.

5.3. Conclusion

The security of regulatory Human Resource Information System (rHRIS) was found to be dependent on the environment on which the system is deployed as different Boards and Councils attained different scores on compliance to the recommended best practices. The study further established that the organization that has implemented an elaborate security policy scored fairly well in all aspects.

The study therefore recommends adoption and implementation of a standard security plan so as to deploy a common security approach in order to attain the same level of compliance and hence similar security operational environment for the system.

The outcome of this study shall be relevant to The existing Boards and Councils who will use the SWOT analysis (Appendix II) to determine the areas of priority in implementing the security plan.

The upcoming Kenyan and regional Boards and Councils and health ministries that are yet to adopt the rHRIS for their data processing can use the proposed security plan as a guide to proactive approach in information system security.

5.4. Further Research

The study suggests that a further study on system vulnerability as this would give an insight as to how the Boards and Councils gauge themselves in terms of security. The study also recommends testing of the security plan to ascertain the feasibility of its implementation.

REFERENCES

1. AHWF (2012). Africa Health Workforce Observatory-Human Resources for Health Country Profile Kenya

2. Boehmer, W., (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001, Second International Conference on Emerging Security Information, Systems and Technologies

3. Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J., Rance, S., (2007). An Introductory overview of ITIL V3. The UK Chapter of the itSMF.

4. Clark, J., Robinson, J. (2013). 7 stages of advanced threats. Princeton, New Jersey: Information security media group.

5. Clark, J., Thacker, N. (2013). Next generation threats:the best defence. Princeton, New Jersey: Information security media group.

6. Crisofari, A., Hodges, C. (2011). Proceedings of the First National Human Resources for Health (HRH) Conference in Kenya-Conference.

7. CISPP (2008) California Office of Information Security and Privacy Protection Information Security Program Guide for state agencies.

8. EIF (2004). European Interoperability Framework for pan-European e-Government Services, European Commission.

9. Gillies, A., (2011). Improving the quality of information security management systems with ISO27000, The TQM Journal, 23(4), pp.367 – 376

10. HRHIS (2009). Human Resources for Health Information Systems: a fact finding study in Zambia and Ethiopia

11. ITGI (2007). IT Governance Institute, COBIT 4.1 Excerpt, Executive summary framework.

12. JTC, (2007). ISO/IEC Joint Technical Committee, International standards,Information technology-Security techniques— code of practise for Security management ISO/IEC27002.

13. Krause, M. Tipton, H.F. (n.d.). Handbook of information security management:Access Control. Retrieved from https://www.cccure.org.

14. Liao, K.H., Chueh, H.E., (2012). An Evaluation Model Of Information Security Management Of Medical Staff, International Journal of Innovative Computing, Information and Control, 8(11), pp 7865 - 7873

15. Lindström , J., Hägerfors, A., (2009). A model for explaining strategic it- and information security to senior management, International Journal of Public Information Systems, vol 1

16. McQuide, P.A., Matte R, Spero J.C. (2011). Human Resources for Health, 9(6)

17. ME (2011). Second annual progress report on implemenattion of the first medium term plan (2008-2012) of Kenya vision 2030, M&E directorate Government of Kenya.

18. Motorola (2010). Information Assurance services:user role in information security. Motorola Corporation.

19. Oltsik, J., Kao, K., Gahm, J., (2012). Security Management and Operations. Enterprise Security Group.

20. Skyler (2011). Retrieved from Introduction to risk management process according to NIST: http://securityreliks.securegossip.com/2011/01/introduction-to-the-risk-assessment-process-according-to-nist/#sthash.INxxZ01r.dpuf

21. Soares, D., Amaral, L., (2011). Information Systems Interoperability in Public Administration. Journal of Theoretical and Applied Electronic Commerce Research , 32.

22. Swanson, M., Bowen, P., Phillips, A.W., Gallup, D., Lynes, D. (2010). NIST special publication 800-34,Contingency Planning Guide for Federal Information Systems.

23. Tashi , I. Ghernaouti-Hallie , S., (2007). ISO Security Standards as a Leverage on IT Security Management, Proceedings of the Americas Conference on Information Systems (AMCIS), Association for Information Systems AIS Electronic Library (AISeL), pp 1 - 12

24. Thiagarajan, V. (2003). Information security management Audit checklist. SANS Institute.

25. Wiander, T. (2007). ISO/IEC 17799 Standard's Intended Usage and Actual Use by the Practitioners, Proceedings of the Americas Conference on Information Systems (AMCIS), Association for Information Systems AIS Electronic Library (AISeL), pp 615 – 621

26. http://riftvalleyhealth.blogspot.com/2012/09/web-based-management-of-health-workforce.html

27. http://www.cdc.gov/

28. http://www.heath.go.ke

29. http://www.human-resources-health.com/content/9/1/6

30. http://www.who.int/en/

31. http://www.vision2030.go.ke/

APPENDIX I: PROPOSED rHRIS SECURITY PLAN

Proposed Information Security Plan for Regulatory Human Resource Information System (rHRIS)

The Board/Council:

Date:

Contact:

Introduction

This security plan applies to the health regulatory agencies in Kenya using the rHRIS to manage health workforce data in areas of training and practice namely:

Nursing Council of Kenya

Kenya Medical Practitioners and Dentists Board

Kenya Medical Laboratory Technicians and Technologists Board

Clinical Officers Council

Pharmacy and Poisons Board

Kenya Nutritionists and Dieticians Institute

Radiation Protection Board and Society of Radiographers Kenya

Public Health Officers and Technicians Council

The plan is to guide in undertaking interventions that assure security of the sensitive data that the agencies handle.

Terms and Definitions

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always be appropriately secured.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including

policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

Asset - anything that contains, disseminates or processes information and has value to the Board/Council
Control - means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
Information security preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved
Policy - overall intention and direction as formally expressed by management
Risk- the likelihood of a threat agent taking advantage of vulnerability and the resulting business impact
Risk assessment - overall process of risk analysis and risk evaluation
Risk evaluation - process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk management - coordinated activities to direct and control the the Board/Council with regard to risk
Threat - a potential cause of an unwanted incident, which may result in harm to a system or the the Board/Council
Vulnerability a weakness of an asset or group of assets that can be exploited by one or more threats

Roles and Responsibilities

Information Security Officer Responsible for information security in the organization, for reducing risk exposure, and for ensuring the Board/Council's activities do not introduce undue risk to the enterprise. The officer also is responsible for ensuring compliance with state enterprise security policies, standards, and security initiatives.
Incident Response Point of Contact Responsible for receiving incident complaints, communicating with organization Incident Response Team and coordinating organization actions in response to an information security incident.
Information System Owner responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

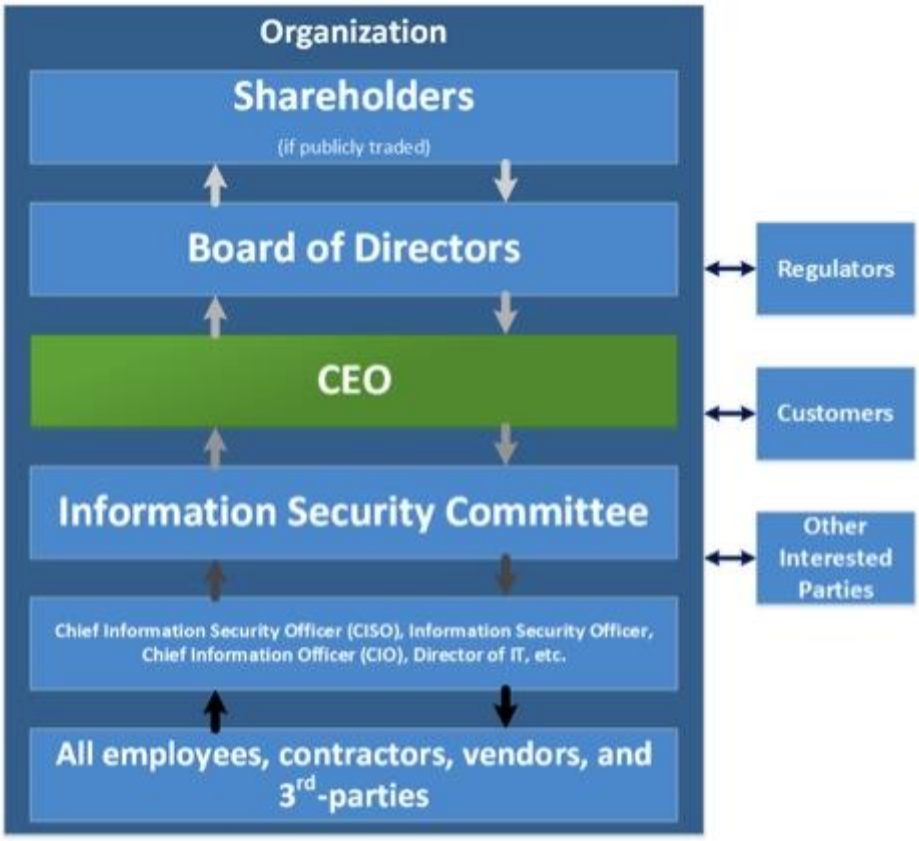
Information Owner Responsible for creating initial information classification, controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.

User Responsible for complying with the provisions of policies, procedures and practices.

Security Program

Information security is a business issue. The objective is to identify, assess and take steps to avoid or mitigate risk to the Board/Council information assets. Governance is an essential component for the long-term strategy and direction of an organization with respect to the security policies and risk management program. Governance requires executive management involvement, approval, and ongoing support. It also requires an organizational structure that provides an appropriate venue to inform and advise executive, business and information technology management on security issues and acceptable risk levels.

The Governance structure shall comprise an executive committee of representatives from IT, human resources, legal, contracts, business services (system users), procurement and other key stakeholder areas.



The following shall be the key Information security goals:

Undertake Business continuity planning

Conduct risk management, audit and assessment

Ensure privacy of all information

In order to implement and properly maintain a robust information security function, the security team shall undertake the following:

Understanding the Board/Council's information security requirements and the need to establish policy and objectives for information security;

Implementing and operating controls to manage the Board/Council's information security risks in the context of overall business risks;

Ensuring all users of the Board/Council information assets are aware of their responsibilities in protecting those assets;

Monitoring and reviewing the performance and effectiveness of information security policies and controls; and

Continual improvement based on assessment, measurement, and changes that affect risk.

Security Components

Risk Management

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Risk management is critical to successfully implement and maintain a secure environment. Risk assessments shall identify, quantify, and prioritize risks against the Board/Council criteria for risk acceptance and objectives. The results shall guide and determine appropriate action and priorities for managing information security risks and for implementing controls needed to protect information assets.

Risk management shall entail the following steps as part of a risk assessment:

Identify the risks

Identify the Board/Council assets and the associated information owners

Identify the threats to those assets

Identify the vulnerabilities that might be exploited by the threats

Identify the impacts that losses of confidentiality, integrity and availability may have on the assets

Analyze and evaluate the risks

Assess the business impacts on the the Board/Council that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of those assets

Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented

Estimate the level of risks

Determine whether the risks are acceptable

Identify and evaluate options for the treatment of risk

Apply appropriate controls

Accept the risks

Avoid the risks

Transfer the associated business risks to other parties

Select control objectives and controls for the treatment of risks

Security Policy

The objective of information security policy is to provide management direction and support for information security in accordance with the Board/Council's business requirements and governing laws and regulations. Information security policies shall be approved by management, and published and communicated to all employees and relevant external parties. These policies will set out an approach to managing information security and will align with relevant statewide policies.

Information security policies shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Each policy shall have an owner who has approved management responsibility for the development, review, and evaluation of the policy.

Reviews shall include assessing opportunities for improvement of the information security policies and approach to managing information security in response to changes to the Board/Council's environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

Security Policy objectives

_____

_____

_____

Organization of Information Security

Information security shall be managed within the Board/Council. Management shall approve information security policies, assign security roles, and coordinate and review the implementation of security across the Board/Council. Information security shall be coordinated across different parts of the Board/Council with relevant roles and job functions. Information security responsibilities will be clearly defined and communicated. Security of the Board/Council's information assets and information technology that are accessed, processed, communicated to, or managed by external parties will be maintained.

Asset Management

The objective of asset management is to achieve and maintain appropriate protection of assets. All the Board/Council assets shall be identified. Owners of information assets shall be identified and have

responsibility for identifying the classification of those assets and maintenance of appropriate controls. To ensure information receives an appropriate level of protection, information shall be classified to indicate the sensitivity and expected degree of protection for handling. Rules for acceptable use of information and information assets will be identified, documented, and implemented.

Asset management objectives

_____

_____

_____

Human Resources Security

All employees, volunteers, contractors, and third party users of the information and information assets shall understand their responsibilities and be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse. Security responsibilities shall be addressed prior to employment in position descriptions and any associated terms and conditions of employment. Where appropriate, all candidates for employment, volunteer work, contractors, and third party users shall be adequately screened, especially for roles that require access to sensitive information. Management is responsible to ensure security is applied through an individual's employment with the Board/Council.

The following measures may be taken to consideration in employment of a new employee or engagement of an external party:

Background checks

Use of non-disclosure agreements

Signing of policies

Detailed job descriptions

All employees and, where relevant, volunteers, contractors and third party users shall receive appropriate awareness training and regular updates on policies and procedures as relevant for their job function.

Steps:

Identify the relevant training needs by conducting a survey to develop topics to be covered and who to be trained.

Provide orientation for all new employees for sensitization and awareness creation

Develop procedures to ensure an employee's, volunteer's, contractor's or third party's exit is managed and the return of all equipment and removal of all access rights are completed.

Physical and Environmental Security

The objective of physical and environment security is to prevent unauthorized physical access, damage, theft, compromise, and interference to information and facilities. Locations housing critical or sensitive information or information assets shall be secured with appropriate security barriers and entry controls. They shall be physically protected from unauthorized access, damage and interference. Secure areas shall be protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Security shall be applied to off-site equipment. All equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal in compliance with statewide policies.

Communications and Operations Management

As a starting point, establish responsibilities and procedures for the management and operation of all information processing facilities. This shall include:

Segregation of duties where appropriate, to reduce the risk of negligent of deliberate system or information misuse.

Prevention and detection of the introduction of malicious code and unauthorized mobile code to protect the integrity of software and information.

Control of media to prevent unauthorized disclosure, modification, removal or destruction of information assets, and interruption to business activities.

Establish procedures for handling and storing information to protect information from unauthorized disclosure or misuse.

Develop a formal exchange policy for exchange of sensitive information and software with other agencies and organizations.

Monitor and record information security events to detect unauthorized access to the Board/Council information and information systems.

Access Control

Access to information, information systems, information processing facilities, and business processes should be controlled on the basis of business and security requirements.The following steps shall be useful in realizing this objective:

Develop formal procedures to control access rights to information, information systems, and services to prevent unauthorized access.

Make users aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords.

Make users aware of their responsibilities to ensure unattended equipment has appropriate protection.

Develop a clear desk policy for papers and removable storage devices and implement a clear screen policy especially in work areas accessible by the public.

Information Systems Acquisition, Development and Maintenance

Access to system files and program source code should be controlled and information technology projects and support activities conducted in a secure manner. Technical vulnerability management should be implemented with measurements taken to confirm effectiveness.

The Board/Council shall:

Develop standard system development life cycle methodology for consistency in acquisition

Undertake vulnerability self assessments periodically

Undertake system penetration tests periodically

Information Security Incident Management

Information security incidents should be communicated in a manner allowing timely corrective action to be taken.

Steps:

Establish an incident response team with clear roles and responsibilities

Develop formal incident reporting and escalation procedures and communicate them to all users.

Establish responsibilities and procedures to handle information security incidents once they have been reported.

Make users aware of their role in incident reporting

Develop users' capacity to respond to incidents e.g by having trainings on remedial actions

Business Continuity Management

The objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

The Board/Council should establish a business continuity management process to minimize the impact on the organization and recover from loss of information assets to an acceptable level through a combination of preventive and recovery controls.

Steps:

Establish a working team with clear responsibilities, the team should consist members from various departments/ operation units

Develop a strategy on business continuity

Define the roles and responsibilities and frequency of reviews

Seek management approval of the strategy

Sensitize users on the strategy

Implement the strategy

Compliance

The design, operation, use, and management of information and information assets are subject to statutory, regulatory, and contractual security requirements. Compliance with legal requirements is necessary to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. Legal requirements include, but are not limited to: national and Board/Council policy, regulations, contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information.

Controls should be established to maximize the effectiveness of the information systems audit process.

Implementation

The Board/ Council should form a technical working group to review the security plan and assess feasibility of implementation. The group should include representatives from all departments.

Approval

By: _____ _____

Name, title Date

By: _____ _____

Name, title Date

By: _____ _____

Name, title Date

APPENDIX II: SWOT ANALYSIS

rHRIS SWOT ANALYSIS

OVERVIEW

This document outlines the current information system security status in terms of administrative, technological and physical controls that have been implemented by summarizing the regulatory Human resource Information System (rHRIS) security status findings for all Boards and Councils.

STRENGTHS

KMLTTB

KMLTTB exhibited the following strengths:

- ✓ Presence of an elaborate draft IT Policy
- ✓ Good asset management and policy on information classification
- ✓ Manned reception and locked server rooms
- ✓ Separation of development and operational facilities
- ✓ Proper IS acquisition, development and maintenance procedure

NCK

NCK exhibited the following strengths:

- ✓ Approved, published and implemented elaborate IT policy
- ✓ Proper organization of information security with diverse representation in coordination of security activities
- ✓ Good inventory management and policy on information classification
- ✓ Good employment procedures with screening of employees and signing of non disclosure agreements.
- ✓ Proper physical and environmental security
- ✓ Documented and implemented change management procedure

WEAKNESSES

This section outlines aspects of the regulatory Human Resource Information System that put it at risk and therefore need to be improved.

Kenya Medical Laboratory Technicians and Technologists Board (KMLTTB)

KMLTTB exhibited the following areas of weakness in its security controls:

- ✓ IT policy not approved hence cannot be published and implemented making it difficult to enforce security.

- ✓ Security activities coordinated soley by IT personnel, this leads to lack of ownership and put the organization at risk.
- ✓ Lack of job descriptions, approved standard operating procedures and human resource security management procedures. The employees cannot be held legally accountable since they are yet to sign any agreements on security.
- ✓ No risk identification has been undertaken so far. The organization is therefore not prepared for active defence.
- ✓ Lack of a business continuity plan, implying that the organization has no strategy in the event of disaster.
- ✓ Backups never tested hence there is no assurance that the system can be restored in case of any failures

Nursing Council of Kenya (NCK)

NCK Backups have never tested, this can results in operation failure in the event of a disaster as the organization is not assured of the reliability of the backup

Clinical Officers Council (COC)

COC has the following security weaknesses

- ✓ Lack of an IT policy
- ✓ Backups never tested, this can result in operation failure in the event of a disaster as the organization is not assured of the reliability of the backup
- ✓ Lack of a business continuity plan

Medical Practitioners and Dentists Board (MPDB)

The following are the weaknesses of the MPDB system security:

- ✓ Lack of an IT policy
- ✓ Backups never tested, this can results in operation failure in the event of a disaster as the organization is not assured of the reliability of the backup

APPENDIX III: TARGETED RESEARCH RESPONDENTS

Listed by Organization, Category and Office titles

Organization	Category	Title
Nursing Council Of Kenya(NCK)	Management(1)	Deputy C.E.O/ Registrar
	Heads of departments(5)	HOD Standards & Ethics HOD Education HOD Examination HOD registration HOD Finance
	Users within departments(10)	Standards Officer, Education Officer, Education assistant, Examination Officer, Registration Officer, Registration Assistant-retention, Registration assistant- private practice
	ICT Personnel (1)	ICT Officer
Kenya Medical Laboratory Technicians and Technologists Board (KMLTTB)	Management (1)	CEO & Registrar
	Heads of Department and users within departments (6)	HOD Education Registration assistant-Personnel Registration Assistant-Facilities Registration Assistant- Exams Indexing Officer PR Officer
	ICT Personnel (1)	ICT Officer
Medical Practitioners and Dentist Board (MPDB)	Management (1)	CEO
	HODs and other users within the departments (4)	Senior Licensing Officer Licensing Officer CPD Officer Data Officer
	ICT Personnel(1)	ICT Officer
Clinical Officers Council(COC)	Management (1)	CEO/Registrar
	HODs and other users within the departments (3) ICT Personnel (1)	Education Officer Registration Officer Standards Officer
Emory Project	Technical Personnel(2)	System programmers (2)

APPENDIX IV: MANAGEMENT INTERVIEW GUIDE

Reference	Audit area, objective and question
Section	Audit Question
Review of Informational Security Policy	Are you aware of the existence of an IT Policy? □YES □NO Is the policy published? □YES □NO Has the policy been reviewed? □YES □NO What informed the review?
Authorization process for information processing facilities	Do you give approval before any system is implemented? □YES □NO If **Yes**, Why do you think it is necessary to do so? _____ Is there a defined process for approvals? □YES □NO If **No**, do you think it is necessary to outline the process? □YES □NO
Reporting information security events	Have you ever received a security incident report? □YES □NO In what format? A)hard copy report B)oral C)electronic notification D)Other(please specify_____ Which of the above formats is most preferable? □A □B □C Please state why
Responsibilities and procedures	What role did you or do you play in response to information security incidents. _____
Business continuity planning framework	Is there an official documented business continuity plan? □YES □NO If **No**, what interventions would you undertake in the event of a disaster? _____
Compliance with security policies and standards	What actions do you take to ensure IT policy implementation? _____
Personnel screening & employment	Do you undertake background verification checks for all candidates for employment, contractors and third party users? □YES □NO Which of these aspects do you take to consideration: *please tick appropriately* □ Character reference □ Confirmation of claimed academic and professional qualifications □ Independent identity checks □ Other(please specify)_____ Do employees, contractors and third party users sign confidentiality or non-disclosure agreement as part of their initial terms and conditions of operation? □YES □NO
General	Do you consider your information to be secure? □YES □NO Please give reasons for your answer above:_____ _____
Data	Have you embraced data for decision making? □YES □NO If No,Why?_____ If Yes, What major decisions have you made based on your data? _____ To what extent would your decisions be affected if the data was corrupted? □Extremely □Slightly □Not at all □No idea
Information sharing	Are there instances of data requests? □YES □NO Is there a formal procedure for information sharing? □YES □NO What role do you play in release of data? _____

APPENDIX V: USER QUESTIONNAIRE

Research Title: Security in health workforce information systems: case of regulatory health workforce information system.

The purpose of this study is to assess level of security in the health workforce information system and develop a security plan for effective data protection.

Reference	Audit area, objective and question
Section	Audit Question
IT Policy	Are you aware of the existence of an IT Policy?□YES □NO Is the policy published? □YES □NO
Terms and conditions of employment	Are you required to sign confidentiality or non-disclosure agreement as part of your contract?□YES □NO
Information security awareness, education and training	Have you received any security awareness training, updates on organizational policies and procedures that pertain to your work?□YES □NO
Information sensitivity	Is the information you deal with categorized?□YES □NO If **yes**, please state the categories_____
Segregation of duties	Do you have job descriptions? □YES □NO Are your duties and responsibilities segregated? □YES □NO If **No**, how do you think this would affect information security? _____ Does the Information system segregate your user roles?□YES □NO
User Password Management	Is there a formal process for allocation and reallocation of usernames and password? □YES □NO Do you sign a statement to keep your password confidential?□YES □NO
Password use	How do you create your passwords, Are their security mechanism in choosing a password e. g must be 8 characters? □YES □NO
Unattended user equipment	Are you aware of the security requirements and procedures in protecting unattended equipment e.g idle computers? □YES □NO Please enlist some that you are aware of: _____
Reporting security weaknesses	Are you required to report any information system weakness?□YES □NO Have you ever reported any? □YES □NO If **yes**, in what format?? **A)**hard copy report **B)**oral **C)**electronic notification **D)**Other(*pleasespecify*)_____ Which of the above formats is most preferable? □A □B □C Please state why_____
Protection of organizational records	How do you enforce information security? A)Not sharing system passwords B)Protecting physical documents If **B** or both, how do you account for physical document access? _____ Do you have procedures for physical document destruction? □YES □NO

APPENDIX VI: GAP ANALYSIS APPLICABILITY MATRIX

Section	Audit Question	Applicability
Information security policy		
Information security policy document	is there an Information security policy	Dr
	is the policy approved by the management	User
	is the policy published and communicated to all employees	Dr
	does the policy state management commitment	Dr
	is the organizational approach to managing information clearly set out	M
Review of Informational Security Policy	Whether the Information Security Policy is reviewed at planned intervals, or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.	M
	Whether the Information Security policy has an owner, who has approved management responsibility for development, review and evaluation of the security policy.	Dr
	Whether any defined Information Security Policy review procedures exist and do they include requirements for the management review.	Dr
	Whether the results of the management review are taken into account.	Dr
	Whether management approval is obtained for the revised policy.	Dr
Internal Organization		
Management commitment to information security	Whether management demonstrates active support for security measures within the organization. This can be done via clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities.	M
Information security coordination	Whether information security activities are coordinated by representatives from diverse parts of the organization, with pertinent roles and responsibilities.	It
Allocation of information security responsibilities	Whether responsibilities for the protection of individual assets, and for carrying out specific security processes, were clearly identified and defined.	It
Authorization process for information processing facilities	Whether management authorization process is defined and implemented for any new information processing facility within the organization.	It

Confidentiality agreements	Whether the organization's need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed.	It
	Does this address the requirement to protect the confidential information using legal enforceable terms	It
Contact with authorities	Whether there exists a procedure that describes when, and by whom: relevant authorities such as Law enforcement, fire department etc., should be contacted, and how the incident should be reported.	It
Contact with special interest groups	Whether appropriate contacts with special interest groups or other specialist security forums, and professional associations are maintained.	Dr
Independent review of information security	Whether the organization's approach to managing information security, and its implementation, is reviewed independently at planned intervals, or when major changes to security implementation occur.	Dr, It, M
External Parties		
Identification of risks related to external parties	Whether risks to the organization's information and information processing facility, from a process involving external party access, is identified and appropriate control measures implemented before granting access.	Dr
Addressing security when dealing with customers	Whether all identified security requirements are fulfilled before granting customer access to the organization's information or assets.	Dr
Addressing Security in third party agreements	Whether the agreement with third parties, involving accessing, processing, communicating or managing the organization's information or information processing facility, or introducing products or services to information processing facility, complies with all appropriate security requirements.	It
Responsibility for assets		
Inventory of assets	Whether all assets are identified and an inventory or register is maintained with all the important assets.	It
Ownership of assets	Whether each asset identified has an owner, a defined and agreed-upon security classification, and access restrictions that are periodically reviewed.	It
Acceptable use of assets	Whether regulations for acceptable use of information and assets associated with an information processing facility were identified, documented and implemented.	It
Information classification		
Classification guidelines	Whether the information is classified in terms of its value, legal requirements, sensitivity and criticality to the organization.	It

Information labelling and handling	Whether an appropriate set of procedures are defined for information labelling and handling, in accordance with the classification scheme adopted by the organization.	Dr
Prior to employment		
Roles and responsibilities	Whether employee security roles and responsibilities, contractors and third party users were defined and documented in accordance with the organization's information security policy.	It,Dr
	Were the roles and responsibilities defined and clearly communicated to job candidates during the pre-employment process	Dr
Screening	Whether background verification checks for all candidates for employment, contractors, and third party users were carried out in accordance to the relevant regulations.	
	Does the check include character reference, confirmation of claimed academic and professional qualifications and independent identity checks	Dr
Terms and conditions of employment	Whether employee, contractors and third party users are asked to sign confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment contract.	Dr
	Whether this agreement covers the information security responsibility of the organization and the employee, third party users and contractors.	Dr
During employment		
Management responsibilities	Whether the management requires employees, contractors and third party users to apply security in accordance with the established policies and procedures of the organization.	Dr
Information security awareness, education and training	Whether all employees in the organization, and where relevant, contractors and third party users, receive appropriate security awareness training and regular updates in organizational policies and procedures as it pertains to their job function.	Dr, User
Disciplinary process	Whether there is a formal disciplinary process for the employees who have committed a security breach.	User
Termination or change of employment		
Termination responsibilities	Whether responsibilities for performing employment termination, or change of employment, are clearly defined and assigned.	U
Return of assets	Whether there is a process in place that ensures all employees, contractors and third party users surrender all of the organization's assets in their possession upon termination of their employment, contract or agreement.	Dr

Removal of access rights	Whether access rights of all employees, contractors and third party users, to information and information processing facilities, will be removed upon termination of their employment, contract or agreement, or will be adjusted upon change.	It
Secure Areas		
Physical Security Perimeter	Whether a physical border security facility has been implemented to protect the information processing service.	
Physical entry Controls	Whether entry controls are in place to allow only authorized personnel into various areas within the organization.	Dr
Securing Offices, rooms and facilities	Whether the rooms, which have the information processing service, are locked or have lockable cabinets or safes.	Dr
Protecting against external and environmental threats	Whether the physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster should be designed and applied.	It
	Whether there is any potential threat from neighbouring premises.	It
Working in Secure Areas	Whether physical protection and guidelines for working in secure areas is designed and implemented.	O
Public access delivery and loading areas	Whether the delivery, loading, and other areas where unauthorized persons may enter the premises are controlled, and information processing facilities are isolated, to avoid unauthorized access.	O
Equipment Security		
Equipment siting protection	Whether the equipment is protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	O
Supporting utilities	Whether the equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	O
	Whether permanence of power supplies, such as a multiple feed, an Uninterruptible Power Supply (ups), a backup generator, etc. are being utilized.	O,It
Cabling Security	Whether the power and telecommunications cable, carrying data or supporting information services, is protected from interception or damage.	Dr,It
	Whether there are any additional security controls in place for sensitive or critical information.	O
Equipment Maintenance	Whether the equipment is correctly maintained to ensure its continued availability and integrity.	It
	Whether the equipment is maintained, as per the supplier's recommended service intervals and specifications.	It

	Whether the maintenance is carried out only by authorized personnel.	O
	Whether logs are maintained with all suspected or actual faults and all preventive and corrective measures.	
	Whether appropriate controls are implemented while sending equipment off premises.	It
	Are the equipment covered by insurance and the insurance requirements satisfied	It
Securing of equipment off-premises	Whether risks were assessed with regards to any equipment usage outside an organization's premises, and mitigation controls implemented.	It
	Whether the usage of an information processing facility outside the organization has been authorized by the management.	Users
Secure disposal or re-use of equipment	Whether all equipment, containing storage media, is checked to ensure that any sensitive information or licensed software is physically destroyed, or securely over-written, prior to disposal or reuse.	It
Removal of property	Whether any controls are in place so that equipment, information and software is not taken off-site without prior authorization.	Dr ,O
Operational Procedures And Responsibilities		
Documented Operating procedures	Whether the operating procedure is documented, maintained and available to all users who need it.	Dr,O
	Whether such procedures are treated as formal documents, and therefore any changes made need management authorization.	Dr,O
Change management	Whether all changes to information processing facilities and systems are controlled.	It
Segregation of duties	Whether duties and areas of responsibility are separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services.	It,Dr
Separation of development, test and operational facilities	Whether the development and testing facilities are isolated from operational facilities. For example, development and production software should be run on different computers. Where necessary, development and production networks should be kept separate from each other.	It
Third party service delivery management		
Service delivery	Whether measures are taken to ensure that the security controls, service definitions and delivery levels, included in the third party service delivery agreement, are implemented, operated and maintained by a third party.	

Monitoring and review of third party services	Whether the services, reports and records provided by third party are regularly monitored and reviewed.	
	Whether audita are conducted on the above third party services, reports and records, on regular interval.	Dr,O
Managing changes to third party services	Whether changes to provision of services, including maintaining and improving existing information security policies, procedures and controls, are managed.	Dr,O,It
	Does this take into account criticality of business systems, processes involved and re-assessment of risks	It
System planning and acceptance		
Capacity Management	Whether the capacity demands are monitored and projections of future capacity requirements are made, to ensure that adequate processing power and storage are available.	Dr,U,It
System acceptance	Whether system acceptance criteria are established for new information systems, upgrades and new versions.	It
	Whether suitable tests were carried out prior to acceptance.	It
Protection against malicious and mobile code		
Controls against malicious code	Whether detection, prevention and recovery controls, to protect against malicious code and appropriate user awareness procedures, were developed and implemented.	It,Dr
Controls against mobile code	Whether only authorized mobile code is used.	It,Dr
	Whether the configuration ensures that authorized mobile code operates according to security policy.	It,Dr
	Whether execution of unauthorized mobile code is prevented.	It
Backup		
Information backup	Whether back-ups of information and software is taken and tested regularly in accordance with the agreed backup policy.	It,Dr
	Whether all essential information and software can be recovered following a disaster or media failure.	It,Dr
Network Security Management		
Network Controls	Whether the network is adequately managed and controlled, to protect from threats, and to maintain security for the systems and applications using the network, including the information in transit.	It
	Whether controls were implemented to ensure the security of the information in networks, and the protection of the connected services from threats, such as unauthorized access.	It
Security of network services	Whether security features, service levels and management requirements, of all network services, are identified and included in any network services agreement.	It,O

	Whether the ability of the network service provider, to manage agreed services in a secure way, is determined and regularly monitored, and the right to audit is agreed upon.	It
Media handling		
Management of removable media	Whether procedures exist for management of removable media, such as tapes, disks, cassettes, memory cards, and reports.	
	Whether all procedures and authorization levels are clearly defined and documented.	It,O
Disposal of Media	Whether the media that are no longer required are disposed of securely and safely, as per formal procedures.	It,O
Information handling procedures	Whether a procedure exists for handling information storage.	
	Does this procedure address issues, such as information protection, from unauthorized disclosure or misuse	It,O
Security of system documentation	Whether the system documentation is protected against unauthorized access.	It,O
Exchange of Information		
Information exchange policies and procedures	Whether there is a formal exchange policy, procedure and control in place to ensure the protection of information.	It,O
	Does the procedure and control cover using electronic communication facilities for information exchange.	
Exchange agreements	Whether agreements are established concerning exchange of information and software between the organization and external parties.	It,Users
	Whether the security content of the agreement reflects the sensitivity of the business information involved.	It,Dr,Users
Physical Media in transit	Whether media containing information is protected against unauthorized access, misuse or corruption during transportation beyond the organization's physical boundary.	It,O
Electronic Messaging	Whether the information involved in electronic messaging is well protected.	It,O
	(Electronic messaging includes but is not restricted to Email, Electronic Data Interchange, Instant Messaging)	It,O
Business information systems	Whether policies and procedures are developed and enforced to protect information associated with the interconnection of business information systems.	It,O
Electronic Commerce Services		
Electronic Commerce	Whether the information involved in electronic commerce passing over the public network is protected from fraudulent activity, contract dispute, and any unauthorized access or modification.	It,Dr

	Whether Security control such as application of cryptographic controls are taken into consideration.	It,Dr
	Whether electronic commerce arrangements between trading partners include a documented agreement, which commits both parties to the agreed terms of trading, including details of security issues.	It,Dr
On-Line Transactions	Whether information involved in online transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	It,Dr
Publicly available information	Whether the integrity of the publicly available information is protected against any unauthorized modification.	It,Dr
Monitoring		
Audit logging	Whether audit logs recording user activities, exceptions, and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	It,Dr
	Whether appropriate Privacy protection measures are considered in Audit log maintenance.	It,Dr
Monitoring system use	Whether procedures are developed and enforced for monitoring system use for information processing facility.	**It**
	Whether the results of the monitoring activity reviewed regularly.	Na
	Whether the level of monitoring required for individual information processing facility is determined by a risk assessment.	Na
Protection of log information	Whether logging facility and log information are well protected against tampering and unauthorized access.	Na
Administrator and operator logs	Whether system administrator and system operator activities are logged.	It
	Whether the logged activities are reviewed on regular basis.	It
Fault logging	Whether faults are logged analysed and appropriate action taken.	
	Whether level of logging required for individual system are determined by a risk assessment, taking performance degradation into account.	It,Dr
Clock synchronisation	Whether system clocks of all information processing system within the organization or security domain is synchronised with an agreed accurate time source.	It,Dr,O
Business Requirement for Access Control		
Access Control Policy	Whether an access control policy is developed and reviewed based on the business and security requirements.	It,O

	Whether both logical and physical access control are taken into consideration in the policy	It,O
	Whether the users and service providers were given a clear statement of the business requirement to be met by access controls.	It,O
User Access Management		
User Registration	Whether there is any formal user registration and de-registration procedure for granting access to all information systems and services.	It,O
Privilege Management	Whether the allocation and use of any privileges in information system environment is restricted and controlled i.e., Privileges are allocated on need-to-use basis, privileges are allocated only after formal authorization process.	
User Password Management	The allocation and reallocation of passwords should be controlled through a formal management process.	
	Whether the users are asked to sign a statement to keep the password confidential.	
Review of user access rights	Whether there exists a process to review user access rights at regular intervals. Example: Special privilege review every 3 months, normal privileges every 6 moths.	It,Dr
User Responsibilities		
Password use	Whether there are any security practice in place to guide users in selecting and maintaining secure passwords.	It,Dr
Unattended user equipment	Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment. .	Dr
Clear desk and clear screen policy	Whether the organisation has adopted clear desk policy with regards to papers and removable storage media	It,Dr
	Whether the organisation has adopted clear screen policy with regards to information processing facility	It,U
Network Access Control		
Policy on use of network services	Whether users are provided with access only to the services that they have been specifically authorized to use.	It,U
	Whether there exists a policy that does address concerns relating to networks and network services.	Dr
User authentication for external connections	Whether appropriate authentication mechanism is used to control access by remote users.	It,U
Equipment identification in networks	Whether automatic equipment identification is considered as a means to authenticate connections from specific locations and equipment.	It,U

Remote diagnostic and configuration port protection	Whether physical and logical access to diagnostic ports are securely controlled i.e., protected by a security mechanism.	
Segregation in networks	Whether groups of information services, users and information systems are segregated on networks.	It,Dr
	Whether the network (where business partner's and/ or third parties need access to information system) is segregated using perimeter security mechanisms such as firewalls.	It,Dr
	Whether consideration is made to segregation of wireless networks from internal and private networks.	It
Network connection control	Whether there exists an access control policy which states network connection control for shared networks, especially for those extend across organization's boundaries.	It,Sc
Network routing control	Whether the access control policy states routing controls are to be implemented for networks.	It,Dr
	Whether the routing controls are based on the positive source and destination identification mechanism.	It
Operating system access control		
Secure log-on procedures	Whether access to operating system is controlled by secure log-on procedure.	It,O
User identification and authentication	Whether unique identifier (user ID) is provided to every user such as operators, system administrators and all other staff including technical.	It,O
	Whether suitable authentication technique is chosen to substantiate the claimed identity of user.	It,O
	Whether generic user accounts are supplied only under exceptional circumstances where there is a clear business benefit. Additional controls may be necessary to maintain accountability.	It,O
Password management system	Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.,	It,Dr
Use of system utilities	Whether the utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.	It,Dr
Session time-out	Whether inactive session is shutdown after a defined period of inactivity.	It,Dr
Limitation of connection time	Whether there exists restriction on connection time for high-risk applications. This type of set up should be considered for sensitive applications for which the terminals are installed in high-risk locations.	It,O
Application and Information Access Control		

Information access restriction	Whether access to information and application system functions by users and support personnel is restricted in accordance with the defined access control policy.	It,O
Sensitive system isolation	Whether sensitive systems are provided with dedicated (isolated) computing environment such as running on a dedicated computer, share resources only with trusted application systems, etc.,	It,O
Mobile Computing and teleworking		
Mobile computing and communications	Whether a formal policy is in place, and appropriate security measures are adopted to protect against the risk of using mobile computing and communication facilities.	It,O
	Whether risks such as working in unprotected environment is taken into account by Mobile computing policy.	Dr
Security requirements of information systems		
Security requirements analysis and specification	Whether security requirements for new information systems and enhancement to existing information system specify the requirements for security controls.	It,Dr
	Whether the Security requirements and controls identified reflects the business value of information assets involved and the consequence from failure of Security.	It,Dr
	Whether system requirements for information security and processes for implementing security is integrated in the early stages of information system projects.	It,Dr
Correct processing in applications		
Input data validation	Whether data input to application system is validated to ensure that it is correct and appropriate.	It,Dr
	Whether the controls such as: Different types of inputs to check for error messages, Procedures for responding to validation errors, defining responsibilities of all personnel involved in data input process etc., are considered.	Sc
Control of internal processing	Whether validation checks are incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	Sc
	Whether the design and implementation of applications ensure that the risks of processing failures leading to a loss of integrity are minimised.	Dr
Message integrity	Whether requirements for ensuring and protecting message integrity in applications are identified, and appropriate controls identified and implemented.	Dr
	Whether an security risk assessment was carried out to determine if message integrity is required, and to identify the most appropriate method of implementation.	It,Dr

Output data validation	Whether the data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances.	Sc
Cryptographic controls		
Policy on use of cryptographic controls	Whether the organization has Policy on use of cryptographic controls for protection of information. .	It, Sc
	Whether the policy is successfully implemented.	It
	Whether the cryptographic policy does consider the management approach towards the use of cryptographic controls, risk assessment results to identify required level of protection, key management methods and various standards for effective implementation	It
Key management	Whether key management is in place to support the organizations use of cryptographic techniques.	It
	Whether cryptographic keys are protected against modification, loss, and destruction.	It
	Whether secret keys and private keys are protected against unauthorized disclosure.	It
	Whether equipments used to generate, store keys are physically protected.	O
	Whether the Key management system is based on agreed set of standards, procedures and secure methods.	It, Dr
Security of system files		
Control of operational software	Whether there are any procedures in place to control installation of software on operational systems. (This is to minimise the risk of corruption of operational systems.)	It,Dr
Protection of system test data	Whether system test data is protected and controlled.	It, M
	Whether use of personal information or any sensitive information for testing operational database is shunned.	It
Access Control to program source code	Whether strict controls are in place to restrict access to program source libraries.	It
Security in development and support processes		
Change control procedures	Whether there is strict control procedure in place over implementation of changes to the information system. (This is to minimise the corruption of information system.)	
	Whether this procedure addresses need for risk assessment, analysis of impacts of changes,	It,O
Technical review of applications after operating system changes	Whether there is process or procedure in place to review and test business critical applications for adverse impact on organizational operations or security after the change to Operating Systems.	It,Dr,O
Restriction on changes to software packages	Whether modifications to software package is discouraged and/ or limited to necessary changes.	It,Dr,O

	Whether all changes are strictly controlled.	Dr
Information leakage	Whether controls are in place to prevent information leakage.	Dr
	Whether controls such as scanning of outbound media, regular monitoring of personnel and system activities permitted under local legislation, monitoring resource usage are considered.	Dr
Outsourced software development	Whether the outsourced software development is supervised and monitored by the organization.	Dr
	Whether points such as: Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect Trojan code etc., are considered.	It,Dr
Technical Vulnerability Management		
Control of technical vulnerabilities	Whether timely information about technical vulnerabilities of information systems being used is obtained.	It
	Whether the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to mitigate the associated risk.	It
Reporting information security events and weaknesses		
Reporting information security events	Whether information security events are reported through appropriate management channels as quickly as possible.	It
	Whether formal information security event reporting procedure, Incident response and escalation procedure is developed and implemented.	It
Reporting security weaknesses	Whether there exists a procedure that ensures all employees of information systems and services are required to note and report any observed or suspected security weakness in the system or services.	It
Management of information security incidents and improvements		
Responsibilities and procedures	Whether management responsibilities and procedures were established to ensure quick, effective and orderly response to information security incidents.	Dr
	Whether monitoring of systems, alerts and vulnerabilities are used to detect information security incidents.	It
	Whether the objective of information security incident management is agreed with the management.	It,U,M
Learning from information security incidents	Whether there is a mechanism in place to identify and quantify the type, volume and costs of information security incidents.	It,Dr
	Whether the information gained from the evaluation of the past information security incidents are used to identify recurring or high impact incidents.	It, Dr, U

Collection of evidence	Whether follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal).	M
	Whether evidence relating to the incident are collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	M
	Whether internal procedures are developed and followed when collecting and presenting evidence for the purpose of disciplinary action within the organization.	It
Information security aspects of business continuity management		
Including information security in the business continuity management process	Whether there is a managed process in place that addresses the information security requirements for developing and maintaining business continuity throughout the organization.	It
	Whether this process understands the risks the organization is facing, identify business critical assets, identify incident impacts, consider the implementation of additional preventative controls and documenting the business continuity plans addressing the security requirements.	It,Dr
Business continuity and risk assessment	Whether events that cause interruption to business process is identified along with the probability and impact of such interruptions and their consequence for information security.	It,U,M
Developing and implementing continuity plans including information security	Whether plans were developed to maintain and restore business operations, ensure availability of information within the required level in the required time frame following an interruption or failure to business processes.	It
	Whether the plan considers identification and agreement of responsibilities, identification of acceptable loss, implementation of recovery and restoration procedure, documentation of procedure and regular testing.	Dr
Business continuity planning framework	Whether there is a single framework of Business continuity plan.	It,Dr
	Whether this framework is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance.	It
	Whether business continuity plan addresses the identified information security requirement.	It,M
Testing, maintaining and re-assessing business continuity plans	Whether Business continuity plans are tested regularly to ensure that they are up to date and effective.	It,Dr
	Whether business continuity plan tests ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when plan is evoked.	Dr
Compliance with legal requirements		

Identification of applicable legislation	Whether all relevant statutory, regulatory, contractual requirements and organizational approach to meet the requirements were explicitly defined and documented for each information system and organization.	It,Dr
	Whether specific controls and individual responsibilities to meet these requirements were defined and documented.	It,U
Intellectual property rights (IPR)	Whether there are procedures to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	*Dr*
	Whether the procedures are well implemented.	*It*
	Whether controls such as: publishing intellectual property rights compliance policy, procedures for acquiring software, policy awareness, maintaining proof of ownership, complying with software terms and conditions are considered.	Dr,It,M
Protection of organizational records	Whether important records of the organization is protected from loss destruction and falsification, in accordance with statutory, regulatory, contractual and business requirement.	It
	Whether consideration is given to possibility of deterioration of media used for storage of records.	Dr,It
	Whether data storage systems were chosen so that required data can be retrieved in an acceptable timeframe and format, depending on requirements to be fulfilled.	It
Data protection and privacy of personal information	Whether data protection and privacy is ensured as per relevant legislation, regulations and if applicable as per the contractual clauses.	It
Prevention of misuse of information processing facilities	Whether use of information processing facilities for any non-business or unauthorized purpose, without management approval is treated as improper use of the facility.	It,U
	Whether a log-on a warning message is presented on the computer screen prior to log-on. Whether the user has to acknowledge the warning and react appropriately to the message on the screen to continue with the log-on process.	It
	Whether legal advice is taken before implementing any monitoring procedures.	It
Regulation of cryptographic controls	Whether the cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.	It
Compliance with security policies and standards, and technical compliance		
Compliance with security policies and standards	Whether managers ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	It

	Do managers regularly review the compliance of information processing facility within their area of responsibility for compliance with appropriate security policy and procedure	It,M
Technical compliance checking	Whether information systems are regularly checked for compliance with security implementation standards.	It.M
	Whether the technical compliance check is carried out by, or under the supervision of, competent, authorized personnel.	
Information Systems audit considerations		
Information systems audit controls	Whether audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to business process.	M
	Whether the audit requirements, scope are agreed with appropriate management.	It
Protection of information system audit tools	Whether access to information system audit tools such as software or data files are protected to prevent any possible misuse or compromise.	It
	Whether information system audit tools are separated from development and operational systems, unless given an appropriate level of additional protection.	It

KEY:

It-Information Technology

Dr-document review

Sc-System configuration

U-Users

M-Management

O-Observation