ISSN 2320 - 2602

Volume 6 No.3, March 2017

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst01632017.pdf

Information Security Management Framework for E-Government in the Kenyan Public Sector: A Case of the Ministry of Public Service, Youth and Gender Affairs

Beatrice Wairimu Kamau[1], Dr. George Okeyo[2], Dr. Michael Kimwele[3]

[1]Masters of science in computer systems,Kenya,bwairimu05@yahoo.com

[2]Jomo Kenyatta University, Kenya,gokeyo@jkuat.ac.ke

[3]Jomo Kenyatta University, Kenya, mkimwele@jkuat.ac.ke

ABSTRACT

ICT has become an increasingly important factor in facilitation of improved services within the public sector. Employment of e-government systems means more effectiveness, efficiency, accessibility and accountability of the government to their citizens in addition to posing security threat to the disseminated information. Information security is thus a key concern in the establishment to ensure success of e-government systems. However this area in e-government in the Kenyan Public Sector has not been adequately addressed.

In this study the researcher presents a case study of e-government interaction within four of the nine Agencies in the Ministry of Public Service, Youth and Gender and the Information Security Management challenges identified in the implementation. This study was guided by the following objectives; to establish the current status of information security management for e-government in the Kenyan Public Sector, to establish factors that hindered effective information security management in the Public Sector, to develop an improved framework that would address the challenges identified in the implementation, to establish if the developed framework would be applicable in the Kenyan Public Sector. To realize these objectives the study sampled ISOs within the Agencies by use of purposive sampling which is a non-probability sampling technique used in quantitative research. This was done through data collection by use of questionnaires and in-depth interviews. The data was analyzed using the statistical package for social scientists (SPSS) to obtain descriptive statistics in form of frequencies, means and graphs for quantitative results. The findings enhanced the development of a workable framework.

Keywords: E- government, Information, Security, Management, Framework.

1. INTRODUCTION

ICT is a key element of reform efforts that can help dramatically reshape government to improve performance and reduce costs. Furthermore, it has opened a new medium of communication for individuals, business, and government organization, providing more opportunities to communicate and get information in an entirely new way. The recent advancement of internet technologies have made majority of governments around the world to adopt information & communication technologies (ICTs) to provide services towards the agencies ,businesses and citizens more efficiently and effectively [12] .E-government services have brought not only tremendous opportunities but also security challenges; though the implementation and service delivery are heavily guided by e-government maturity models (e-GMM), they lack built-in security services both technical and non-technical [7].

The Kenyan government has been able to put in place a substantial infrastructure to enable the provision of the services through electronic means since the commencement of e-government strategy implementation in 2004; However e-government presents challenges in regards to information security to governments [8] . It is a fact that information security has an important role in mitigating security risks and threats posed to security e-government services while the security improves quality offered and cuts across entire organizations [7]. Therefore, since it requires involvement of employees at all levels, it is imperative that confidentiality, integrity and availability of critical information stored, processed and transmitted between governments, business and citizens become an integral part of e-government services, implementation, delivery and maintenance phases.

The overall objective of this study is to develop an improved information security management framework for e-government services, in the Kenyan Public Sector with consideration of four agencies from the ministry of public service youth and gender affairs as a case study. The framework integrates five information security goals (confidentiality, integrity, availability, authentication and non-repudiation), the control measures that are involved in the mitigation of security threats and breaches, the three levels of management (strategic, functional and operational) that ensure implementation of control measures as well as enhancement of the security goals and information security audit & monitoring to ensure secure e-government services in the Kenyan public sector. The information security management framework was guided by the following questions,

- What is the current status if information security management in the Kenyan public sector?
- What factors hindered effective management of information security practices in the Kenyan public sector?
- How could improvements in the management of information security in the Kenyan public sector be achieved?

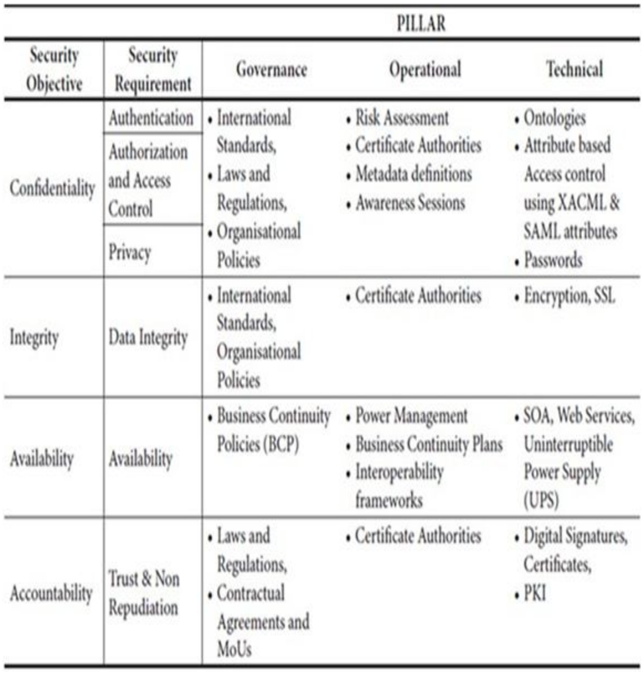
By addressing the above questions through the study the researcher will recommend possible ways to pursue to ensure appropriate management of information security for e-government services in both public and private sectors. The researcher was partly motivated to undertake this study by the increase of security threats and breaches in the Kenyan public sector for the past three years. On the other hand, consideration of the ministry of public service, youth and gender ministry was due to the fact it is one of the largest ministries consisting of nine agencies. This fact was hoped to help get a clear picture of what is experienced in the sector in regards to management of information security. It can therefore be hoped that the findings of this study can readily be used as a drive to enhance good management of information security within the public and private sectors.

2. RELATED WORK

2.1 Information Security Frameworks for E-Government

E-government framework is a guideline used by government organizations and businesses working with the government. Information security is a serious requirement which must be carefully considered .E-government security frameworks facilitate government organizations to effectively offer appropriate secure e-government service [1].

2.1.1. The TOG Framework



		PILLAR		
Security Objective	Security Requirement	Governance	Operational	Technical
Confidentiality	Authentication	• International Standards, • Laws and Regulations, • Organisational Policies	• Risk Assessment • Certificate Authorities • Metadata definitions • Awareness Sessions	• Ontologies • Attribute based Access control using XACML & SAML attributes • Passwords
	Authorization and Access Control			
	Privacy			
Integrity	Data Integrity	• International Standards, Organisational Policies	• Certificate Authorities	• Encryption, SSL
Availability	Availability	• Business Continuity Policies (BCP)	• Power Management • Business Continuity Plans • Interoperability frameworks	• SOA, Web Services, Uninterruptible Power Supply (UPS)
Accountability	Trust & Non Repudiation	• Laws and Regulations, • Contractual Agreements and MoUs	• Certificate Authorities	• Digital Signatures, Certificates, • PKI

Figure 1.TOG framework by [11].

The information security framework is referred to as TOG (Technical, Operational and Governance) framework that recognizes the need for e-Government transactions cognizant of national legislation, policies at the same time comply with organizational policies. The authors' of TOG Framework matched the technical operational and governance pillars with the security objectives and requirements for a sustainable security framework for e-Government.

2.1.2 COBIT 5 Framework

COBIT 5 [3] provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. It helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. Additionally, it enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. Furthermore its principles and enablers are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector. Moreover, it is not prescriptive, but it advocates that enterprises implement governance and management processes such that the key areas are covered, as shown in figure 2.

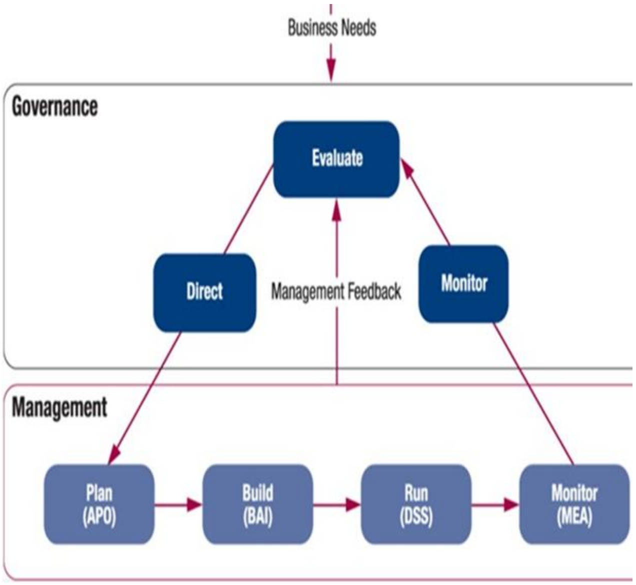


Figure 2. COBIT 5 Governance and Management Key Areas

2.1.3. ISO/IEC 27001

The focal point of ISO 27001[6] is the requirement for planning, implementation, operation and continuous monitoring and improving of process-oriented ISMS. The approach should be aligned with the PDCA cycle (Figure 3)

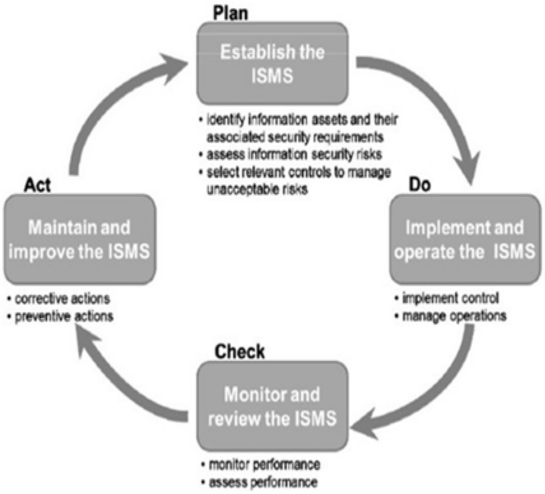

Plan
Establish the ISMS
• identify information assets and their associated security requirements
• assess information security risks
• select relevant controls to manage unacceptable risks
Do
Implement and operate the ISMS
• implement control
• manage operations
Check
Monitor and review the ISMS
• monitor performance
• assess performance
Act
Maintain and improve the ISMS
• corrective actions
• preventive actions

Figure 3.The PDCA cycle

The Plan Phase

This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls.

The Do Phase

This phase includes carrying out everything that was planned during the previous phase.

The Check Phase

The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.

The Act Phase

The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

3. THE PROPOSED INFORMATION SECURITY MANAGEMENT FRAMEWORK

The researcher has developed a framework to enhance the management of information security for e-government services in the Kenyan Public Sector. The framework integrates IS goals, control measures, levels of management and IS audit. Therefore the framework will adopt the name Security Goals, Control Measures, Management and Audit (SECOMA) Framework. The framework informs the user clearly on the different types of control measures that helps in the mitigation of security risks. Additionally it informs on the different levels of management concerned with enhancement of information security.

The information provided in the framework may be likened to that available in COBIT 5 framework [3] that mainly concerns itself with governance and management of IT however; it does not separate operational functions of the framework from management.

COBIT 5 framework treats security goals, information security audit and control measures as management functions but they are operational functions under different levels of management (Strategic, operational and functional level).The SECOMA framework clearly stipulates the functions of the different levels for management of information security in addition to the types of control measures.

The data used to develop the framework were both primary and secondary data. For the primary data, the researcher developed a criterion which was used to filter the research findings and identify the critical factors that are necessary to offer guidance in the development of the proposed framework. The framework is shown in figure 4.

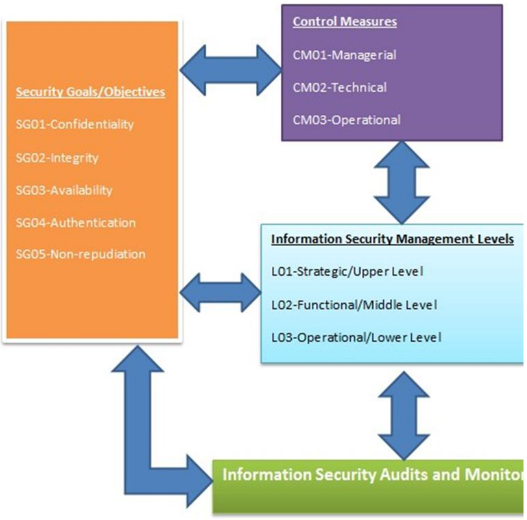

Control Measures
CM01-Managerial
CM02-Technical
CM03-Operational
Security Goals/Objectives
SG01-Confidentiality
SG02-Integrity
SG03-Availability
SG04-Authentication
SG05-Non-repudiation
Information Security Management Levels
L01-Strategic/Upper Level
L02-Functional/Middle Level
L03-Operational/Lower Level
Information Security Audits and Monitor

Figure 4. The SECOMA Framework for e-government services in Kenyan Public Sector.

3.1 Discussion of the framework.

3.1.1. Security goals.

There are three security goals of information and information processing resources that are also referred to as C-I-A triad or information security triad [4]. Additionally,[5] expresses that the CIA triad shows the fundamental goals that must be included in information security measures.

However [2], the authors of "Evolution of the information Security goals from 1960 to today" states that the list of security goals has broadened. Moreover, they stress that information security is also concerned with authentication, accountability, nonrepudiation and reliability. Additionally, the set of goals is neither fixed nor given because security goals are changing over time in response to the evolution of society business needs and ICT. Therefore information security professionals should be alert to the rapid evolution of a valid collection of security goals and be ready to conduct, regularly as an insight for analysis of security issues posed by emerging technology. These include confidentiality, integrity, availability, authentication and non-repudiation.

3.1.3. Control Measures

The tremendous grow of technology today exposes the computer systems to a lot of security threats. This means that information is likewise threated, hence organizations are called to take initiatives in the implementation of the necessary controls i.e. safeguards or counter measures to avoid, detect, counteract of minimize security risks to information. These controls can vary in nature but fundamentally they are ways of protecting the security objectives of information. They include Managerial (Administrative) Control Measures, Technical Control Measures and Operational (Functional/Physical) Control Measures.

3.1.4. Information Security Management Levels

In the context of information security management, the word management usually refers to the necessary requirements and/or obligations to effectively initiate, plan, execute, monitor and control information security activities across the organization, in an effort to successfully achieve organizational security objectives; and to protect the organization from all potential threats, hence making it an indispensable process [3].The levels include Strategic/Upper Level, Functional/Middle Level, Operational/Lower Level [9].

3.1.2. Information security Audits and Monitoring.

To maintain operational assurance, organizations use two basic methods: system audits and monitoring [10]. Therefore the two terms are used loosely within the computer security community and often overlap. They further state that a system audit is a one-time or periodic event to evaluate security while monitoring refers to an ongoing activity that examines either the system or the users.

4. FRAMEWORK VALIDATION

To evaluate the usefulness of the developed framework the researcher considered the recommendations given by the participants who were purposefully selected from two of the Ministry of Public Service Youth and Gender Affairs Agencies that were sampled during data collection. The following are the factors, to which the respondents gave positive responses leading to the conclusion that the framework is viable,

- The developed framework is clearly understandable to the intended user.
- The framework will improve ISM for e-government services.
- Tasks highlighted in the framework apply in real-life situations.
- The framework is aligned with current security standards and practices.
- The framework is flexible enough to deal with possible ISM challenges.

5. CONCLUSION

The main goal of this study was to develop an improved information security management framework for e-government services in the Kenyan public sector. In this respect, a framework was developed which adopted the name Security Goals, Control Measures, Management and Audit (SECOMA) Framework.

Another goal was to establish the current status of information security for e-government in the Kenyan public sector. The findings revealed that most organizations in the public sector do not ensure awareness and training in relation to information security to their employees. Further findings revealed that most information security threats were as a result of malicious software whereas the only means used to mitigate the threats were antivirus software and firewalls.

Another goal of this study was to establish factors that hindered the effective management of information security in the Kenyan Public Sector. The study findings revealed that passwords are the most commonly used means of user authentication which may not be termed sufficient means for protection purposes whereas the only means used as physical control measures are backup files (&documentations) and backup power . The study also revealed that most organizations do not observe the information security objectives nor protect information from unauthorized user or modification. Further findings revealed that most organization only involve the operational level of information security management cycle neglecting the strategic and functional levels which need to be incorporated for efficient execution of the e-government services. The findings also revealed that most organizations lack the necessary personnel to guarantee effective and independent execution of information security audits and monitoring in addition to lack of a functional information security management framework that would enhance e-government services.

6. RECOMMENDATIONS FOR FUTURE RESEARCH

The proposed framework for information security management was only designed for the Kenyan public sector; this opens an opportunity for the same research to be applied for other sectors including the East African community at large. The study established that biometric access controls are not employed in the public sector. This calls for further studies to establish the most appropriate form of biometrics to be employed which may include finger prints, hand prints, voice pattern, signature samples and retinal scans. The study established that only antivirus software and firewall methods were used for threat mitigation. The researcher suggests further study to establish the effectiveness of encryption, two-way authentication and intrusion detection system if they were to be utilized in the public sector.

REFERENCES

[1] Alwi N. & Ihmouda R. (2014): A Comparative Analysis of e-government security frameworks Social-Technical Security Aspect.

[2] Cherdantseva Y. & Hilton J. (2012)The Evolution of Information Security Goals from The 1960s to Today.

[3] COBIT 5 (ISACA,2012): A business Framework for governance & Management of enterprise IT.

[4] Filippone L.(2013): Fundamental Security Concepts.

[5] Henderson A.(2016):Panmore.com/the-CIA-triad-confident-integrity-availability;accessed on 14/10/2016 at 5.25pm.

[6] ISO/IEC 27001(2013): Information technology — Security techniques — Information security management systems — Requirements.

[7] Karokola G.R. (2010) A Framework For Securing E-Government Services: The Case Of Tanzania.

[8] Oyieyo W.O. (2010): E-Government Security: Information Security Management Model For Public Administration In Kenya.

[9] Raggad B.G (2010): Information Security Management Concepts and Practice.CRC press-Tylor & Francis group.

[10] Swanson M. & Guttman B. (1996): General Accepted Principles and Practices for Securing Information Technology Systems.

[11] Wangwe, Eloff, Venter (2012):A Sustainable Information Security Framework For E-Government – Case of Tanzania.

[12] Waziri M.D. &Yonah Z.O.(2014),Towards a Secure Maturity Model for Protecting e-Government Services in Tanzania: A stakeholders View.