International Journal of Research in Engineering, Science and Management
Volume 6, Issue 11, November 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Enhancing Information Security Management Systems for Improved Service Delivery in Kenyan Local Authorities

Vincent Motochi[1*], Waliaro Apollo Madi[2]
[1]ICT Officer, Department of ICT, Kakamega County Service Board, Kakamega, Kenya
[2]Lecturer, Department of Computer Science, Masinde Muliro University of Science and Technology, Kakamega, Kenya

***Abstract*: Applying information systems security is strategically important to maintaining overall business continuity and indirectly enforcing quality services in many sectors. However, the process of effectively implementing information security management systems in local authorities is challenging to security practitioners. Management models such as CIA, ACIA and ISMS which were indented to address the security issues have proved ineffective with the emerging new information systems. Anew approach is needed to address this emerging security challenges. The objective of this study involved developing a model unique to local authorities operating in Kenya. The researcher employed a survey using a mixture of qualitative and quantitative methods since this was a problem centered study in order to provide a comprehensive analysis of the study problem. The data was collected using interview schedules and questionnaires. Data was analyzed using descriptive statistics frequencies, mode, and standard deviation. The study developed a model for managing information systems security issues.**

***Keywords*: security model, information systems security, service delivery, local authorities.**

1. Introduction

The chief objective of Information Security Management is to implement the appropriate measurements in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. In doing so, Information Security Management will enable implementing the desirable qualitative characteristics of the services offered by the organization (i.e., availability of services, preservation of data confidentiality and integrity etc.). These organizations have many reasons for addressing information security very seriously. Legal and regulatory requirements which aim at protecting sensitive or personal data as well as general public security requirements impel them to devote the utmost attention and priority to information security risks. Under these circumstances the development and implementation of a separate and independent management process namely an Information Security Management System is the one and only alternative.

A. Statement of the Problem

Although information security management systems in the public sector is a function recognized as necessary, the actual priority allocated to security is not always commensurate with importance. Further, there is often conflict with exactly how specific management of security practices should occur and how it impacts with the associated work practices and service delivery. Often an overall lack of a coordinated security approach could exacerbate this situation highlighting the problem of gaining acceptance of security in a diversified and prior competitive environment. An approach was required that provided a meaningful methodology for progressing information security management systems on service delivery in the public sector, a challenged environment where competing priorities exist. The approach sought to determine the status of ISMS in local authorities, evaluated key issues influencing service delivery and thereafter developed an improved version of ISMS model that fits local authorities. Therefore, evaluating of information security management systems and its impact on service delivery to the general public could be improved was a key focus of this study.

B. Significance of the Study

The relevance of this study work was of significant value to the local authority sector.

It represented the first comprehensive study into contemporary and relevant issues facing this sector. The study provided an insightful examination of the status of play, highlighted issues and deficiencies in service delivery, and provided an explanation of how improvements could be achieved. The timing of the study reflected an early attempt to begin to 'baseline' knowledge on security management. This in essence brought a step further in placing security at a level where the public sector had anticipated an improved understanding and awareness of security as an increasingly prominent theme in operations. Moreover, scholars also find this study a useful addition to the existing body of knowledge besides serving as a benchmark for further study.

*Corresponding author: awaliaro@mmust.ac.ke

C. Improving ISMS Models

1) Confidentiality, Integrity and Availability (CIA) Model

This model is now too simple to describe more than the basic elements of security. For example, elements that the CIA model does not represent include accountability and responsibility (Von Solms 2000).

Lacking in the CIA model is the new requirement to have a business focus incorporated by an accountability and responsibility orientation (Whitson 2003).

2) Accountability, Confidentiality, Integrity and Availability (ACIA) Model:

A deficiency of this model is the fact that it keeps quiet on issues concerning risk management as per Andersen (2001) and Von Solms (1999). Also lacks user authentication, authorization, and reliability which are very important aspects of information systems security (Dhillon, 1999; Siponen and Oinas-Kukkonen, 2007; May and Lane. 2006; Ruighaver et al., 2007).

3) Information Security Management Systems Model

ISMS is not linked to appropriate organizational context and supported by appropriate policy. However, while they provide the framework for operation it is not clear how these standards should be converted to policy and practical operations, and further, whether attempts to do so have been effective within local authorities; and the standards only provides guidelines and not actual tailored solutions for organizations, there is no specifications that an auditor or implementer could refer to.

It is therefore important to understand that for an information security management system to be effective, it still requires the ability to make effective management decisions about organizations activities (Cohen 1999). This means that even if the ISMS is developed that reflects best practice, is based on internationally accepted standards such as 17799, and is properly resourced, it will only be effective if it is supported by organization's processes.

2. Study Methodology

The approach the researcher used in this study was supported by a mixture of methods (qualitative and quantitative) since this was a problem centered study. A descriptive survey was selected because it provided an accurate portray or account of the characteristics, for example behaviour, opinions, abilities, and knowledge of a particular individual, situation or group. This design was chosen to meet the objectives of the study.

A. Target Population

The study was conducted in the five local authorities within Kakamega County Government of approximately 300 members from county councils, municipal councils and town councils running information systems (MOLG Strategic plan 2008), and was stratified into the council employees. The sampling method the researcher employed for the study was purposive sampling and as such, it is a non-probability sampling. The main data collection tools included questionnaires,interview schedules, analysis of documentation, and observation in the real-world setting of security in Kakamega County. The mixed methods approach allowed for both text and statistical analyses of data, and permitted more flexibility when designing questions for survey interviews. Descriptive statistics and the vital measures of central tendency played a role. Data analysis was performed on the interview transcripts using qualitative methods that conformed broadly to thematic qualitative data analysis involving cross referencing of data to identify emerging themes and patterns.

3. Findings

The results of the interviews provide rich information regarding the questions.

A. How could improvements in information security management systems be achieved and enhance service delivery?

A structured and coordinated approach was needed to improve effectiveness of current information security management approaches.

Developing a more structured and coordinated management model for progressing security within the Council community was seen as an essential step in delivering improved security management. An integrated, structured approach was cited as necessary to improve security management throughout Kakamega County local authorities.

Table 1
Summary

Influencing Factors	Respondents (%)
Structured management Approach	15
Security Awareness and Communication	11
Senior Management Support	16
Funding	16
Cultural Compliance	6
Conflicts in work priorities	4
Reactive Approach	17
Security policy	15

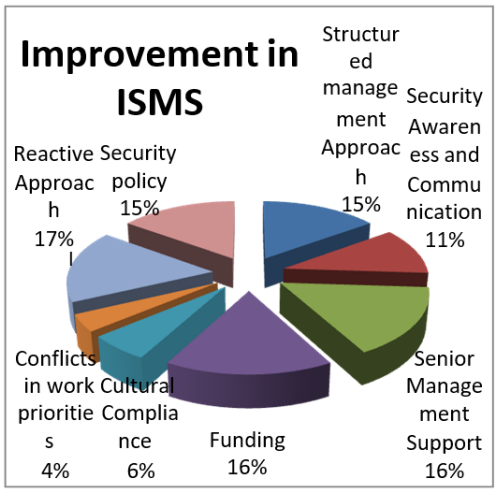

Fig. 1. Areas that will improve ISMS

4. Discussion

A. Improving Information Systems Security Policy

There is wide agreement that good information security policy is the foundation for an organization's information security (Baskerville and Siponon, 2002). An effective

information security policy is the cornerstone of an information security management program (Peltier, 2004, Maynard and Ruighaver, 2002). Importantly, the policy establishes the concept that information is an asset of the organization, and that members of the organization have a responsibility to protect it (Peltier, 2004, Maynard and Ruighaver, 2002). It follows therefore that assessing the end product (the status of actual security), should also be accompanied by an evaluation of the quality of the security policy process. This includes both the development and maintenance of security policy.

Development of security policy has involved considerable emphasis on examining assets to be protected, followed by revolving policy around principles and actions required to protect those assets. However, an approach was required where not only the assets are included, but an understanding of and contribution towards developing a culture of compliance within the organization was required. This necessitates developing policy with an organizational context in mind.

General characteristics of a policy should ensure that it is short and easy to read, with general length of between one and five pages being adequate. If the policy is too long, people is not read it.

The policy should be reviewed on a regular and consistent basis, and updated, if necessary, in line with major organizational, regulatory or technological changes. The policy needs to be realistic, achievable, must be able to be practically implemented and also needs to be enforceable.

Information security policy formulation is often reported to be an ad hoc process. It is suggested therefore that information security policies should be developed with the guidance of information security management standards and guidelines (Gaskell, 2000; Baskerville and Siponen, 2002; Hone and Eloff, 2002a).

B. Improving Information Systems

1) Security Awareness

In proposing a conceptual foundation for organizational information security awareness, Siponen (2000) suggests that the occurrences of human error in information security need to be mitigated by a security awareness programme based on or reflecting a framework similar to the one proposed by NIST (1998). The NIST guideline recommends: identify programme scope, goals and objectives; identify training staff and identify target audiences, motivate management and employees; administer the programme, maintain the programme; and finally evaluate the programme.

Siponen (2000) maintains that security awareness issues is not well-understood, resulting in ineffective security guidelines or programs in practice. The need for a structured security awareness programme would appear to be reasonably epidemic. Siponen (2000) is critical of existing approaches to information security awareness and education, citing them as being too descriptive (and therefore not accomplishment oriented). What is needed, according to Siponen, is the creation of an information security awareness programme through a systematic approach. The aim of the programme is ultimately an effort to minimize end-user errors and non- compliance. 66% of participants feel that there needs to be a strategic, targeted and continuous program in place to increase awareness in councils, one that is adequately funded and resourced. Users resist change if they could not see the benefits, or the process is difficult or time consuming. It is also necessary to balance awareness raising activities with transparent technology processes that minimize requirements for end user awareness. A classic example is using network admission control for end user workstation registration instead of relying on end user diligence and awareness to use antivirus software and maintain operating system updates.

C. Improving Information Systems

1) Security Compliance

Despite security being a recognized issue, many organizations lack a full understanding of what they should be doing and how to go about implementing security as shown in Table. A lack of availability and comprehensiveness of security guidelines and standards is not the issue as these is already available to a large extent. A critical characteristic of security is that many aspects of security is transparent until a breach occurs (Furnell et al., 2000). Therefore, appropriate recognition of security must be brought to the attention of the organization and acted upon. Security must be viewed as a multi-faceted problem which requires a comprehensive solution to encompass physical, procedural and logical forms of protection. As a result, a range of expertise is required to progress appropriate solutions (Furnell et al., 2000). Improved governance, being adequately funded and resourced and increased awareness and training as shown in Table, are rated as the top three areas necessary to make major improvements in compliance with security. Within a structured approach, having the right framework not only applied to management of processes, but also technology controls including standards for systems development, operating standards, best practices and the 'nuts and bolts' of tightening security controls.

Measurement of security and aiming for a certain level of compliance is also seen as desirable. Couldnon (2006) suggests that ensuring compliance necessarily revolves around one fundamental concept 'Is policies being followed the way I expect them to be?'

Promoting a culture of compliance and achieving even small changes in attitude and behaviour may take years, according to Gaunt (1998), highlighting the necessity for these efforts to be channeled through a security strategy. Cultural compliance therefore needs to be examined from the perspective of having an appropriate security strategy in place.

Obtaining compliance with information security faces a number of challenges that Nosworthy (2000) describes as 'balancing factors' between risk and control. In many cases Councils have the belief that because it hasn't happened to them than it ever will. This type of mindset, unless proven otherwise, makes committing to information security seem an unnecessary expense.

In developing a culture of compliance, standards is also likely to provide an important function by fostering a sense of identity, as activities is directed towards achievement of the standard, according to May (2003). The pragmatism that standards embody must however be relevant and be applied

appropriately across the organization from top management down. While top management support for information security is seen as essential, so is cross organizational understanding of security risks and gaps.

D. ISO/IEC 27001: ISMS Model

The ISMS standards specify a framework for organizations to manage information security aspects of their business, and if necessary to demonstrate to other parties (e.g., business partners, auditors, customers, suppliers) their ability to manage information security. Published by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC), it specifies a risk-based security management system that is designed to ensure that organizations select and operate adequate and proportionate (i.e., cost effective) security controls to protect information assets. It uses the 'plan-do-check-act (improve)' model. The model is summarized in the table and figure.

Table 4
Control

Others	Description
Control Objectives – 39	Appendix IV
Controls - 133	Appendix IV

1) ISMS Implementation (PDCA)

Plan, Do, Check, Act is to be applied to structure all ISMS processes. Figure 2, illustrates how an ISMS takes the information security requirements and expectations of the interested parties and, through the necessary actions and processes, produces information security outcomes that meets those requirements and expectations.

2) Model Weakness

Organizations look at this as an internationally accepted standard or model but they find it hard to copy paste it to their level in a way that would fit. Therefore, organizations have to customize it with a few additions and subtractions where necessary. Moreover, it leaves some areas which are crucial out.

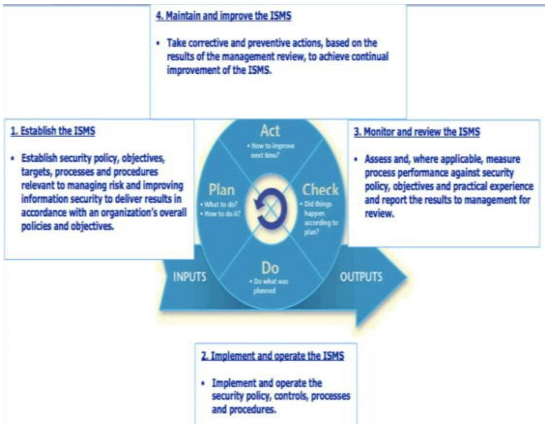

Fig. 2. ISMS model while implementing as described by ISO

E. Improved ISMS Model

A detailed analysis of the data collected through the survey resulted in the generation of emerging themes, patterns and theories consistent with the analysis methodology. The proposed security practitioner's model represents a synthesis of these emergent themes, patterns and theories. Essentially the model seeks to provide a way to think about the fundamental challenges faced by the security practitioner in progressing security implementation within Councils in Kakamega County. The major challenges could be thought of as requiring a way of understanding not so much what to implement, but how to think about implementation in order to progress it within the institution.

Table 2
ISMS model's mandatory parts

Mandatory parts of the Model	Description
Information Security Management System	– General requirements – Establishing and managing the ISMS (e.g. Risk Assessment) – Documentation Requirements
Management Responsibility	– Management Commitment – Resource Management (e.g., Training, Awareness)
Management Review of the ISMS	– Review Input (e.g., Audits, Measurement, Recommendations) – Review Output (e.g., Update Risk Treatment Plan, New Recourses)
ISMS Improvement	– Continual Improvement – Corrective Action – Preventive Action

Table 3
Model domain areas

Domain	Description
Security policy	Management direction
Organization of information security	Governance of information security
Asset management	Inventory and classification of information assets
Human resources security	Security aspects for employees joining, moving and leaving an organization
Physical and environmental security	Protection of the computer facilities
Communications & operations management	Management of technical security controls in systems and networks
Access control	Restriction of access rights to networks, systems, applications, functions and data
IS acquisition, development and maintenance	Building security into applications
Information security incident management	Anticipating and responding appropriately to information security breaches
Business continuity management	Protecting, maintaining and recovering business-critical processes and systems
Compliance	Ensuring conformance with information security policies, standards, laws and regulations

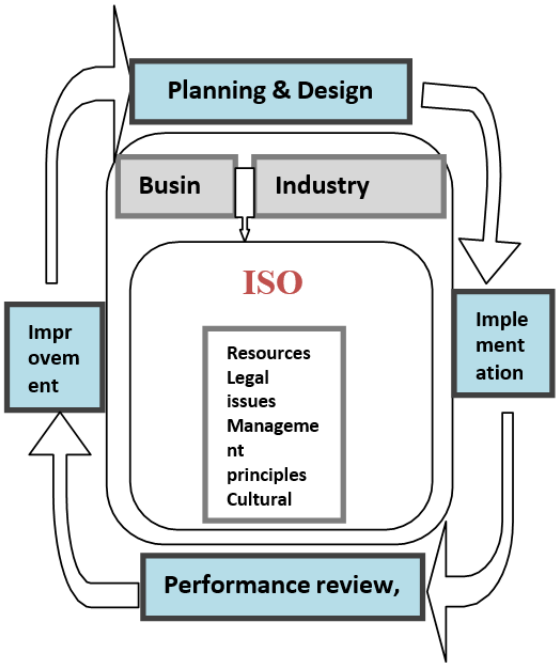

Fig. 3. An enhanced ISMS model

1) Justification for Security Practitioner's Management Model

Addressing compliance is but one aspect of keeping information security central to conducting business. A successful information security model also:

a) Incorporates risk-based decision-making processes into day-to-day business activities.
b) Integrates information security into core IT and business practices.
c) Ensures adequate resource allocation for the projects and programs designed to reduce risk.
d) Dedicates resources to focus on key elements of the information security program.

The new model introduced the ISMS into the existing information security program to increase efficiency and improve the ability to consistently repeat processes with greater clarity about responsibilities, improved internal coordination, and efficiency. The ISMS is aligned with the ISO 27001 security control clauses. Aligning the ISMS program elements to the ISO 27001 security control clauses allows the new model to more easily communicate security obligations and risk mitigation strategies to control owners and performers, as well as provide evidence to auditors and customers that the council has a mature and rigorous program for managing information security, one that is continuously improving.

5. Conclusion

A. Summary of Research Outcomes and Recommendations

As with most things viewed in hindsight, the task of this research study was more onerous than first envisaged. Additionally, the process that was undertaken could now be considerably improved via a more refined and specific approach.

This exercise has however demonstrated the valuable potential for surveying and benchmarking security in Councils on a more regular basis.

The results of this research indicate that Councils face a number of challenges in relation to implementing information security in today's environment. A well- developed information security policy underpinning a structured, formalized information security management program was going a long way towards protecting the value that Councils in Kakamega County create. Additionally, senior management has an ever-increasing mandate to consider information security as part of good corporate governance, and to protect the assets of information, including their reputation and image. Increasingly, Councils is recognizing and acting on the fact that information is an asset of strategic importance and that the threats are growing and demand a suitable response.

Finally, the capacity for senior management to set the tone at the top could not be overestimated. For senior management to view information security as a necessity is expected, however for senior management to view security as an enabler takes the topic to a completely new level.

As threats increase, and reliance on information and systems becomes more critical, the need for security could only strengthen. Councils must rise to the challenge.

B. Recommendations

Security practitioners should adopt an enterprise approach to the management of security in an effort to harness greater levels of support from senior management. The management model is designed to further facilitate these specific recommendations.

1) Increasing senior management awareness and understanding of the role of information security in protecting critical assets and therefore as part of good corporate governance.
2) The use of an enterprise based structured security architecture, coordinated and standards-based management approach for security management.
3) Adoption of information security meta- policy using layered abstraction and refinement methods and incorporating international standards-based recommendations for structure and content.
4) Integrating a structured security awareness program that is as automated as possible to ensure increased awareness, education and training amongst the Council community and inclusive of a 'framework and content' structure.
5) Fostering a culture of compliance towards information security through both behaviour and technology. Behavioral aspects incorporate attempting to normalize behaviour through cultural efforts and technology through technology-based policy enforcement.

C. Contributions

This research work is of significant value to the Council sector, as it represents a unique contribution to the security management issues facing Councils in Kakamega County. It also provides an insightful examination on the current status of play, highlights issues and deficiencies, and provides a realistic

recommendation on how improvements insecurity management could be made.

Lastly, this research has brought forward the idea on a wide scale to all involved that security in Councils is a growing concern and needs to be elevated to an appropriate level.

The study also identified the need for benchmarking security in Councils in Kakamega County which has the potential as a future research project.

References

[1] Anderson, P.W., (2001), Information systems security Governance, *Information systems security Technical Report*, vol. 6, no. 3, pp. 60-70.
[2] ASIS International. (2002). "The General Security Risk Assessment Guidelines," ASIS International, Alexandria, Virginia, USA.
[3] Bayuk, (1996) Security through Process Management. (Web Document)
[4] Baskerville, R. and M. Siponen (2002). An Information systems security Meta-Policy for Emergent Organisations. Logistics Information Management, 15(5/6): 337-346.
[5] County Council of Kakamega (2006) Strategic plan – (2006/2010).
[6] Cohen, F. (1999), Managing Network Security: Why it Is Done That way. Network Security, vol. 1999, no. 12, 1999, pp. 7-9.