Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View

G. Karokola, S. Kowalski and L. Yngström

Department of Computer and Systems Sciences
Stockholm University/Royal Institute of Technology
Forum 100, SE-164 40 Kista, Stockholm, Sweden
e-mail: {karokola, stewart, louise}@dsv.su.se

Abstract

The paper proposes a comprehensive information security maturity model (ISMM) that addresses both technical and socio/non-technical security aspects. The model is intended for securing e-government services (implementation and service delivery) in an emerging and increasing security risk environment. The paper utilizes extensive literature review and survey study approaches. A total of eight existing ISMMs were selected and critically analyzed. Models were then categorized into security awareness, evaluation and management orientations. Based on the model's strengths – three models were selected to undergo further analyses and then synthesized. Each of the three selected models was either from the security awareness, evaluation or management orientations category. To affirm the findings – a survey study was conducted into six government organizations located in Tanzania. The study was structured to a large extent by the security controls adopted from the Security By Consensus (SBC) model. Finally, an ISMM with five critical maturity levels was proposed. The maturity levels were: undefined, defined, managed, controlled and optimized. The papers main contribution is the proposed model that addresses both technical and non-technical security services within the critical maturity levels. Additionally, the paper enhances awareness and understanding on the needs for security in e-government services to stakeholders.

Keywords

e-Government, Information Security, Maturity Model, Security services, Technical and Non-technical security

1. Introduction

Government organisations around the globe have become more dependent on Information and Communication Technology (ICT) for supporting core operations so as to achieve their goals (Dhillon, 2000). Similarly, organisation's critical information has developed into a key strategic asset in a competitive world (Woodhouse, 2008b). e-Government is *"the government-owned or operated systems of information and communication technologies that transform relations with citizens(C), the private sector (B) and other government agencies (G) so as to promote citizens' empowerment, improve government efficiency and service delivery, strengthen accountability and increase transparency"* (WorldBank, 2001). To guide and benchmark a stage-wise e-government implementation and services delivery - several models called "e-Government Maturity Models (eGMMs)" having different

maturity stages were developed by international organizations, consulting firms, academia, and individual researchers (Karokola et al, 2009a, 2010b). A maturity stage in eGMM reflects the level of e-government maturity; degree of technology complexity; degree of systems sophistication; and the level of interaction with users. Also, it offers governments the abilities to measure the progress of e-government implementation (Karokola et al, 2009a, 2010b; WorldBank, 2004). However, the findings from a comparative analysis of eGMMs (Karokola et al, 2009a, 2010b) show that the models were designed with focus on functionalities. They measured more the quantity of e-government implementation and service delivery rather than the quality. Specifically they lacked non-techincal aspects of security in their services models (Karokola et al, 2009a, 2010b). Technical security aspects include hardware and software solutions (Bishop, 2006; McGraw, 2005; Wimmer et al, 2001). Non-technical security aspects include ethical and cultural norms, legal and contractual documentation, administrative and managerial policies, operational and procedural guidelines, and awareness programmes (Henry, 2004; Karokola et al, 2009a, 2010b; Kowalski, 1994; Martins et al, 2002; Woodhouse, 2008b; Yngström, 1996).

Traditionally, interactions between governments (G), businesses (B) and citizens (C) require a physical visit to government offices - posing little threat to the paper based information assets. However, with the advent of e-government services – it has become possible to virtually make e-government services easily accessible and available to more users (World-Bank, 2004). As a result e-government mission-critical information assets are exposed to more security threats. Security threats exploit specific vulnerabilities affecting confidentiality, integrity and availability of e-government critical information assets (Bishop, 2006; Busu, 2004; Grant & Chau, 2005; Lambrinoudakis et al, 2003; McGraw, 2005). Information security is an essential tool for managing security risks in e-government. It ensures confidentiality, integrity and availability of critical information being stored, processed, and transmitted between e-government domains (Bishop, 2006; McGraw, 2005; Zhou & Hu, 2008). When appropriately implemented it creates confidence and trust among e-government users leading to the success of e-government initiatives (West, 2004; Wimmer & Bredow, 2002). There are a number of Information Security Maturity Models (ISMMs) developed to mitigate security risks to the organisations (Dzazali et al, 2009; Fraunhofer, 2005; ISM3, 2007; Rao et al, 2003; Thomson et al, 2006; Woodhouse, 2008a). ISMM is defined as the structured collection of security elements that describes different maturity levels in the organization. Maturity levels are meant for describing different levels of technology and security sophistication that help organizations to easily identify and understand existing security gaps; monitor the progress of security implementation, practices, policies and quality; and monitor security investment, management and organizational audit (Fraunhofer, 2005; ISM3, 2007; Rao et al, 2003). Despite the fact that these models rather measure quality than quantity of services offered, they also lack much of non-technical security services (ISM3, 2007; Lessing, 2008; NIST, 2007; Woodhouse, 2008a).

Being part of on-going research, we explore the existing information security maturity models (ISMMs) and propose a comprehensive ISMM that addresses both technical and non-technical aspects of security services/requirements. The paper is organized as follows: section two presents the research approach. Section three presents extensive literature review on the ISMMs, section four presents analyses of the survey study, and section five proposes the ISMM. Lastly, discussion and conclusion including further research direction is given in section six.

2. Research Approach

This research utilizes Naïve inductivist approach as defined by Alan Chalmers, in Kamiski (1999). Naïve inductivist starts by first observing the phenomenon, and then use these observations for generalizations about the phenomenon from which scientific knowledge/theory can be derived (Kaminski, 1999). The approach is chosen because it gives a deeper understanding of the phenomenon in question (the current security problem in e-government services). Therefore, we conducted an extensive literature review including security standard documents on information security maturity models (ISMMs). A total of eight existing ISMMs were selected and critically analyzed. Models were then categorized into information security management, evaluation and awareness orientations. Based on the model's strengths – three models, one from each category, were selected to undergo further analyses and be synthesized. To affirm the findings – we conducted a survey study. Because this is on-going research work – we needed to maintain consistency and continuity of our previous research study settings (Karokola et al, 2009b; Karokola, 2010a), so, six government organisations located in Tanzania, were surveyed (see section four). The study was structured to a large extent based on the security control structures (technical and non-technical) adopted from the Security By Consensus (SBC) model (Kowalski, 1994).

3. Related Work on Information Security Maturity Models

The selection criteria for the information security maturity models (ISMMs) were: the ISMM must be designed with focus to organizations, must be information security based, and must define security maturity within its levels. Other selection criteria were: models should be highly cited and ranked in the internationally recognized journals and conferences for the past five years, and widely advocated by both practitioners and academia. Based on these criteria the following models were selected: Information security management maturity model (ISM3, 2007), NIST (PRISMA) information security maturity model (NIST, 2002, 2007), Generic security maturity model (GSMM) (Lessing, 2008; Fraunhofer, 2002), Gartner's information security awareness maturity model (GISMM) (Dzazali et al, 2009), and SUNY's information security initiative (Lessing, 2008). Others were: IBM information security framework (IBM-IFM, 2007), Citigroup's information security evaluation maturity model (CitiGroup, 2000), Continuous learning and improvement framework (CLIF) (Rao et al, 2003), and ISMS (Im) – maturity model (Woodhouse, 2008a).

3.1. Analysis of the Selected Information Security Maturity Models

ISM3 consortium (2007) proposed an information security management maturity model (ISM3) with five levels: undefined, defined, managed, controlled and optimized. The model offers a practical and efficient approach to managers and auditors – for evaluating, specifying, implementing and enhancing process oriented information security management systems. The strength of the model is that it includes both coverage and capability maturity levels. In addition, the model development is grounded on the existing security standards, frameworks and best practices such as CMMI, ITIL, ISO 9000, and ISO 17799/27001. The ISM3 can be applied to any organization regardless of its size, context and resources. It gives a clear description of responsibilities for technical/operational personnel – responsible for executing defined goals by means of technical processes; tactical personnel – deals with design and implementation of information security management systems; and strategic personnel – deals with broad goals, coordination, and provision of resources. However, ISM3 does not measure risk or security directly. Metrics are process based measuring activities, scope, effectiveness, efficiency and quality. Every process in ISM3 is assumed to contribute to the goals of information security management. Additionally, the model assumes constant services delivery across all levels of security maturity i.e security risk vs efforts required to mitigate such risk. Furthermore, non-technical or socio security related issues are not sufficiently addressed.

National Institute of Standard and Technology (NIST) (2007) under its program review for information security management assistance (PRISMA) developed a methodology for evaluation information security maturity (ISM) of organisations. The model has five levels, namely: policies, procedures, implementation, testing, and integration. In addition, the model is driven by nine key areas that are divided into strategic and technical aspects. These include: information security management and culture; information security planning; security awareness, training and education; budget and resources; and lifecycle management. Others are: certification and accreditation, critical infrastructure protection, incident and emergency response, and security controls. According to NIST (2002, 2007) higher level of maturity can only be attained if and only if the previous maturity level is attained. This implies that if there is no policy for specific criteria, none of the maturity levels will be attained for the specific criteria. Further, the model is oriented to evaluation and documentation of IT systems, and it does not address adequately aspects of non-technical security services (NIST, 2002, 2007).

Steven Woodhouse (2008a) proposed a unique process maturity model for accessing capability and maturity of processes that affect information security management system (ISMS). The proposed model was named as "ISMS (Im) – maturity capability model". In the study, he argues that the current existing security maturity models can not determine the assessment of lower levels, i.e below level one. In addition, he claims that perception of cultural issues do exists in an organization. To address these issues, he analyzed and compared five security maturity models and came-up with the ISMS (Im) – maturity capability model. The model has nine levels divided

into two main categories: managed processes (from level 1 to 5) and unmanaged process drift (below level 1). Managed processes are: Functional, technical, operational, managed, and strategic. Unmanaged process drift are: Negligent, obstructive, arrogant and subversive. Despite of the model covering organisational cultural issues, the model does not show how security assurance and metrics can be achieved. Due to paper space limitation, full description of other ISMMs such as GISMM (Dzazali et al, 2009), SUNY's ISI (Lessing, 2008), ISF-IBM (2007), and Citi-ISEM (2000) are not given here. But the analysis of their strengths and weaknesses is summarised in table 1 below.

3.2. A Comparative Analysis of Information Security Maturity Models

Based on the detailed analysis of ISMMs presented above, we summarize the findings in table 1 below.

Information Security Maturity Models (ISMM)	Orientation	Limitation to e-Government	Maturity Level Dimensions					
			-3 to 0	1st	2nd	3rd	4th	5th
ISM3 – Information Security Management Maturity Model [ISM3, 2007]	IS Mgt, Risk assessment and Process Integration	Organizational cultural issues,	-	Undefined,	Defined	Managed	Controlled	Optimized
NIST-PRISMA – Information Security Maturity Model [NIST, 2007]	Evaluation and Documentation	Non-technical Security issues		Policies	Procedures	Implementation	Testing	Integrating
GSMM - Generic Security Maturity Model [Lessing, 2008; Neubauer, 2005]	Information Protection	Non-technical Security issues	-	Blind Trusting	Repeatable	Defined	Managed	Maintenance
GISMM - Gartner's Information Security Awareness Maturity Model [Dzazali et al, 2009]	Security Awareness, and Risk Management	Non-technical Security issues	-	Blissful ignorance	Awareness	Corrective	Operations Excellence	
SUNY's ISI - Information Security Initiatives [Lessing, 2008]	Information security protection	Non-technical Security issues	-	Responding to basics	Building protections	Security Programme	Maintaining Security	
ISF-IBM – information Security Framework [IBM-ISF, 2007]	Security gap Analysis	Non-technical Security issues	-	Initial	Basic	Capable	Efficiency	Optimizing
Citi-ISEM - Citigroup's Information Security Evaluation Maturity Model [CitiGroup, 2000]	Security Awareness and Evaluation	Non-technical Security issues	-	Complacency	Acknowledgement	Integration	Common Practice	Continuous Improvement
ISMS (Im) – Maturity Model [Woodhouse, 2008a]	Management Control	Organizational Assurance and metrics	0:Negligent 1:Obstructive 2:Arrogant 3:Subversive	Functional	Technical	Operational	Managed	Strategic

Table 1: A comparative Analysis of Information Security Maturity Models

We summarize the findings from the above analysis as follows:

- Models foundation appear to be based on Systems security engineering capability maturity models (SSE-CMM, 2003) – SSE-CMM gives better foundation for building a security maturity model; Also, models appears to be oriented to three major categories: information security management, evaluation, and awareness;

- Most models appear to consider more of technical security controls than of non-technical ones. Non-technical security controls need to be part of the model design as they play great role in providing security to e-government services; Additionally, other models apart from lacking aspects of non-technical security controls, also lack much of organisational assurance and metrics assessment;
- Models appear to measure more security quality than quantity of offered services (Fraunhofer, 2002; ISM3, 2007; Lessing, 2008; Thomson et al, 2006; Woodhouse, 2008a).

Based on the models' strengths we select one model from each category (management, evaluation and awareness). These were: ISM3 (ISM3, 2007), NIST (PRISMA) (NIST, 2002), and GISMM (Dzazali et al, 2009). Further, we synthesized (Walsh et al, 2005) the selected models and proposed an ISMM with five critical maturity levels (presented in section five). The proposed maturity levels are: *undefined, defined, managed, controlled,* and *optimized*. It should be noted that some of the security control structures (technical and non-technical) came from the Security By Consensus (SBC) model (Kowalski, 1994).

To affirm the proposed model's maturity levels and respective security controls' dimensions – we conducted a survey study (presented in section four).

4. Survey Study

The survey study aimed at affirming the proposed information security maturity levels and their respective security control requirements (technical and non-technical). To maintain consistency and continuity of our previous research study settings (Karokola et al, 2009b, Karokola, 2010a) - we needed to use the same six organisations studied before: *Organisation U:* is a ministry responsible for managing the overall revenue, expenditure and financing of the government; *Organisation V:* is a ministry mandated to effectively administer land and human settlement development services for the betterment of social and economic well being of the society in the country; and *Organisation W*: is a ministry under the President's office responsible for administration of public sector. In her organizational structure it has a unit responsible for coordinating e-government initiatives countrywide. Others were: *Organisation X:* a ministry under the Prime Minister's office charged with instilling good governance to all levels of regional secretariats (RSs) and local government's authorities (LGAs) within the country; *Organisation Y*: is an agency charged with managing all ports and cargo in the country. The agency is now undergoing major upgrading of it's network infrastructures to effectively and efficiently support e-government services delivery; and *Organisation Z:* is an agency responsible for managing the assessment, collection and accounting of all central government revenues. The contacted groups were from different organisational levels: strategic (director of IT / assistant), tactical (IT managers / senior technical staff responsible for e-government) and operational (personnel responsible for implementing and/or managing e-government services). The study was conducted in early March, 2011.

4.1. Questionnaire Preparation, Distribution and Data Collection

Questionnaire preparation: a questionnaire was prepared aimed at gathering stakeholders' views on the proposed ISMM maturity levels and their respective security controls. To be able to comprehensively establish security control requirements – we needed to identify the key security dimensions. So, we adopted security control dimensions (technical and non-technical) from the Security By Consensus Model (SBC) (Kowalski, 1994). Thus, the model's strength is based in its inclusion of both technical and non-technical security controls. The technical security controls are hardware and software solutions, whilst the non-technical security controls include ethical and cultural norms, legal and contractual documentation, administrative and managerial policies, and operational and procedural guidelines (Kowalski, 1994, Yngström, 1996). In addition, we added awareness programmes as part of non-technical security control (Henry, 2004; Karokola et al, 2009a, 2010a, 2010b). Filling in the questionnaire - *Likert scale* (Kothali, 2004) was used for rating the ISMM maturity levels and their respective security controls dimensions requirement. The Likert scale ratings were: Strongly disagree, Disagree, Not sure, Agree, and Strongly agree.

Questionnaire distribution: To test the consistency and validity of our questionnaires – we first sent it to six (n = 6) respondents (one for each organisation) via email. We were able to receive responses from all respondents. The necessary required improvements for the questionnaire were made. Then, the refined questionnaire was distributed to the earlier mentioned organisations via email. The aim was to target one personnel from each level (strategic, tactical and operational) within the organisations.

Data collection: a total of eighteen (n = 18) personnel were contacted, with an average of three (n = 3) personnel from each organisation, whereas a total of 72% responded. Group-wise the responses were: at the strategic level (n = 3), tactical level (n = 4), and operational level (n = 6). The distribution of contacted and responded personnel, organisational wise, is summarised in Table 2 below.

Organization Name	Total Number of Contacted Respondent			Total Number of Respondent		
	Strategic Level	Tactical Level	Operational Level	Strategic Level	Tactical Level	Operational Level
U	1	1	1	1	1	1
V	1	1	1	0	0	1
W	1	1	1	0	1	1
X	1	1	1	1	0	1
Y	1	1	1	0	1	1
Z	1	1	1	1	1	1
Total (n)	**6**	**6**	**6**	**3**	**4**	**6**
	18			**13**		

Table 2: Summary of respondents from each organization

4.2. Data Analysis

Data analysis process was divided into two parts. The first part *analyzes the frequency of acceptability* for the proposed ISMM maturity levels and their respective security controls dimension. The second part *compares the degree of acceptability* among responder's groups (strategic, tactical and operational) for the proposed ISMM maturity stages and their respective security controls dimension.

Acceptability for the proposed ISMM maturity levels and their respective Security Controls dimension*:* figure 1 below depicts a summarized comparative analysis for the acceptability of security controls requirement (technical and non-technical) proposed at each maturity level of an information security model. However, due to paper space limitation – other ratings for those who were either *"Not sure"* or *"Disagree"* are not shown here.

Acceptability for the proposed security controls at maturity level 1 (undefined): acceptability rating for the proposed technical security controls at this level was at 23.1% and 30.8% for both hardware and software technical solutions respectively. Regarding the non-technical security controls – Awareness was rated 100%, suggesting that it is highly recommended. Acceptability rating for other security controls was at 69.2% for both ethical & cultural and legal & contractual. Operation and procedural was rated at 38.5%, suggesting that these security controls have more influence on ensuring secure e-government implementation and service delivery at this maturity level. Figure 1 below shows the acceptability rating in detail.

Acceptability for the proposed security controls at maturity level 2 (defined): there was a significant increase of acceptability rating for the proposed security controls. Technical security controls were rated at 76.9% and 84.6% for hardware and software solutions respectively. Regarding the non-technical security controls - operational & procedural and awareness was highly rates, suggesting that these security controls should be more emphasised. The lowest rated non-technical security controls were ethical and cultural rated at 76.9%. Figure 1 below depicts the analysis in detail.

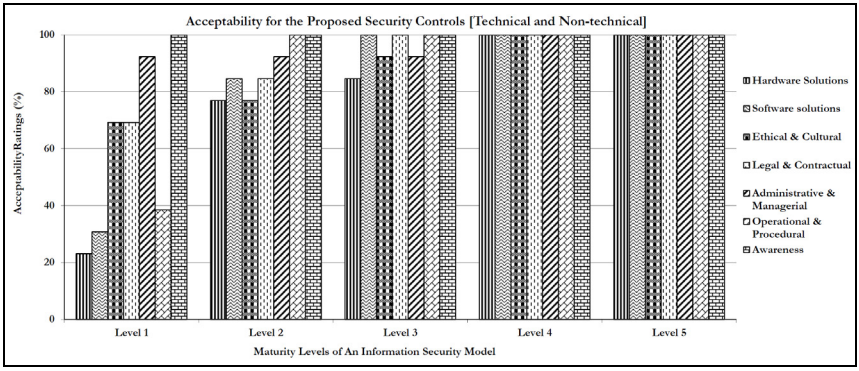

Figure 1: Comparison of Security Control Acceptability (%) for each ISMM Levels

Acceptability for the proposed security controls at maturity level 3 (managed): there was a significant increase of acceptability rate for the proposed security controls. Technical security controls were rated at 84.6% and 100% for both hardware and software solutions respectively. With regards to ethical & cultural and administrative & managerial both were rated at 92.3%. And the rest were rated at 100%. This implies that at maturity level 3 – respondents are expecting e-government implementation and services delivery to be well protected. Figure 1 above shows the details of the analysis.

Acceptability for the proposed security controls at maturity level 4 (controlled) and level 5 (optimized): the proposed security controls at these two levels were rated at 100%. Implying that respondents suggested that the proposed security controls should be at the maximum at both levels. Maturity level 4 is expected to have security controls that are more proactive than reactive in nature. Whilst maturity level 5 is intended to be dealing with new /un-foreseen emerging security risks. Figure 1 above shows the acceptability levels in detail.

Comparison for acceptability of the proposed ISMM maturity levels and their respective security controls among respondent's groups Levels (strategic, tactical and operational): there is a significant variation for the acceptability of security controls among the three group levels, in particular for maturity level 1, 2 and 3 as shown in figure 2 below. Due to paper space limitation – other ratings for *"Not sure"* or *"Disagree"* are not shown here.

Comparison for the acceptability of the proposed security controls at maturity level 1 (undefined): the findings show that there is a significant variation of about 25% for technical solutions among the group levels. Directors preferred to have more technical solutions right from the start, i.e. when e-government service is introduced. This was followed by the managers and operational personnel respectively. Similar findings were observed for non-technical security controls, such as ethical & cultural, legal & contractual, and operational & procedural. This suggests that directors were more concerned with security than other groups, and that they see security as a technical issue. There were no variation for administrative & managerial and awareness security controls, both were rated high as shown in figure 2(a) below.

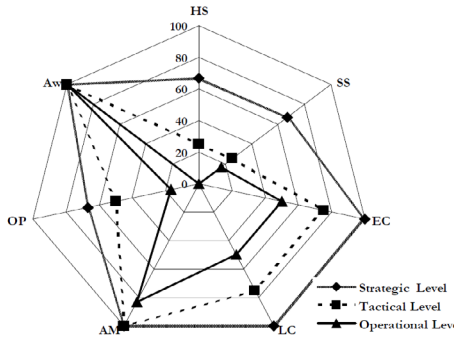

Fig. 2(a): Comparison of acceptability (%) for the Proposed ISM Level 1 security controls

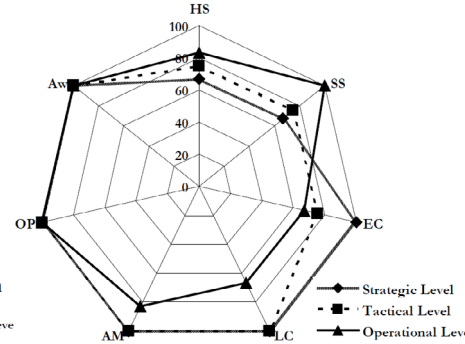

Fig. 2(b): Comparison of acceptability (%) for the Proposed ISM Level 2 security controls

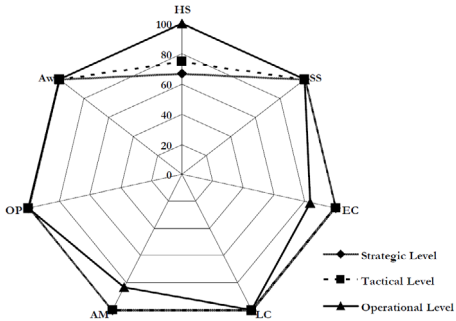

Fig. 2(c): Comparison of acceptability (%) for the Proposed ISM Level 3 security controls

Key terms and Security controls dimension:

AM – Administrative & Managerial
Aw – Awareness
EC – Ethical & Cultural
HS – Hardware Solutions
LC – Legal & Contractual
OP – Operational & Procedural
SS – Software Solutions
ISM – Information Security Maturity

Figure 2: Comparison for the Acceptability of Security Controls for the proposed ISMM among different surveyed organisational groups (Strategic, tactical and operational levels).

Comparison for acceptability of the security controls at maturity level 2 (defined): there is a significant difference of about 12% for technical solutions between directors and managers. At this level managers had a view that the technical solutions should be given more priority than in the previous maturity level. On the other hand, directors had a feeling that technical security controls, at this maturity level, be the same as in the previous level. Similarly, there were significant rating variances between operational personnel and managers of about 8.3% and 25% for hardware and software technical solutions respectively. This suggests that operational personnel were more concerned than managers, and managers were more concern than directors. Regarding the non-technical security controls – directors and managers had similar opinion whereby the proposed security controls were rated high. However, operational personnel gave low ratings for ethical & cultural, legal & contractual, and administrative & managerial. Figure 2(b) above depicts the analysis.

Comparison for acceptability of the security controls at maturity level 3 (managed): there were significant differences for rating of technical security controls, particular for the hardware solutions. Operational personnel rated it high at 100%, whilst managers rated it at 75% and directors at 67%. Regarding the non-technical security controls – rated high by all groups with exception of ethical & cultural and administrative & managerial which was rated at 83.3% by the operational personnel group. This suggests that directors and managers were more concerned than the operational personnel group. Figure 2(c) shows the analysis in detail.

Comparison for acceptability of the security controls at maturity level 4 (controlled) and level 5 (optimised): both security controls were rated high at 100% by all groups for maturity levels 4 and 5 – implying that security control need to be maximized. (However, it should also be noted that, it is important for an organisation to cost-effectively mitigate the associated security risks in e-government services when implementing security controls measures).

5. The Proposed Model

This section presents the proposed information security maturity model (ISMM) for secure e-government services (implementation and service delivery). Basically, the model is based on the findings from the critical analysis of ISMM presented in section three followed by the survey study presented in section four. The following maturity levels with their respective security control dimensions are proposed:

Maturity level 1 (undefined): this is the lowest maturity level of an information security model meant for organizations with low information security targets (IST - refers to security requirements for the given information system or product (CC, 2009; ISM3, 2007)) in a low security risk environment – where process metrics are not compulsory. Security policies may be available. Adequate user awareness are necessary. Security risk reduction from technical and non-technical security threats occur.

Maturity level 2 (defined): the second maturity level is meant for organizations with normal information security targets (IST) in a normal security risk environment. Process metrics may be used but not compulsory. At this level, security policies including awareness, visions, and strategies are reviewed and updated. More security risk reduction from technical and non-technical security threats occurs. Information security is slowly imbedded into the organizational culture.

Maturity level 3 (managed): this is the more advanced level than level 2. It is meant for organizations with high information security targets (IST) in a normal or high security risk environment. Also, high risk reduction from technical and non-technical security threats occurs. At this level process metrics may be used. In addition, security policies including awareness, visions, and strategies are regularly reviewed and updated.

Maturity level 4 (controlled): the fourth maturity level of information security model is meant for organizations with higher information security targets (IST) in a normal or higher security risk environment. Highest security risk reduction from technical and non-technical security threats occurs. Uses of process metrics are compulsory. Information security is embedded into the culture of the organization. Additionally, Security policies, awareness, visions, and strategies are regularly reviewed and updated.

Maturity level 5 (optimized): this is assumed to be the highest maturity level. It is meant for organizations with higher information security targets (IST) in higher security risk environments. Highest security risk reduction from technical and non-technical security threats occurs. Uses of process metrics are compulsory. Like in the previous maturity level – security policies, awareness, visions, and strategies are regularly reviewed and updated. Information security is embedded into the culture of the organization.

We summarize the above maturity levels into a pictorial presentation shown in figure 3 below. The figure shows the maturity levels of an information security model. Maturity level one and level five being the lowest and highest respectively. In addition, the figure shows that as you go up to higher maturity levels security risks increase, consequently more effort is needed to mitigate such security risks.

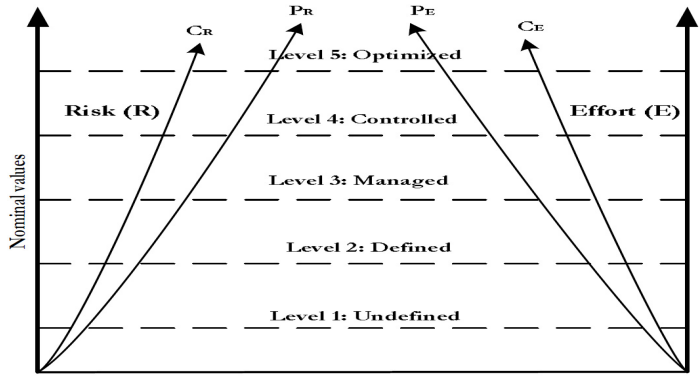

Figure 3: Graph of ISMM showing Maturity levels, Risks and Efforts

Information Security risk is defined as the potential that a given threats will exploit vulnerabilities of an assets or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence (ISO-27k, 2008).

Security threats, in this context, is defined as any circumstance or event with the potential to adversely impact to organization critical assets, through an authorized access, destruction, disclosure, modification of information, and/or denial of service (ISO-27k, 2008). There are three primary steps to perform risk analysis. These are: identifying risks, determining the impact of threats, and balancing the impact of the threats with safeguards (ISO-27k, 2008; NIST, 2002, 2007).

Therefore, from the figure 3 above, we calculate security Risk and Effort required to mitigate security risk:

Security Risk (exposure) = Likelihood (Probability (P_R)) x impact (Consequences (C_R));

= Probability (P_R) x Consequences (C_R);

Security Effort (mitigation) = Likelihood (Probability (P_E)) x impact (Consequences (C_E));

= Probability (P_E) x Consequences (C_E);

Whereas:

- Probability = threats x vulnerability;
- Consequences = $\sum_{i=1}^{n} Consequence_i$

Where i = Consequence of Confidentiality, Integrity or Availability (CIA) of Assets

Note:

Each of the element in figure 3 such as Security Risk (exposure), and Security Effort (E), etc, are divided into technical and non-technical security controls.

Using the proposed approach one can easily determine security risks and efforts needed to mitigate such risks both technical and non-technical related ones.

6. Discussion and Conclusion

Gary McGraw (2005) argued that security should be built into a system from the start, and not be considered once the system is completed. The existing studies show that more efforts are invested in developing technical security services than non-technical security ones. As a result, there exists a wider gap between technical and non-technical security services). In this paper, we proposed a comprehensive ISMM that addresses both technical and non-technical security aspects for secure e-government services. The survey's findings suggests that by using the model, organisations can better understand, define, implement, control, and continuously improve technical and non-technical security services for secure e-government services. Additionally, by using the model organizations should be able to determine their current and plan for future level of maturity, thereby be better able to implement security in the correct order.

As discussed above the focus of most maturity models in e-government maturity seem to be quantity based rather than quality based. By integrating quality based ISMM model with an e-government model organizations can measure both quantity and the quality of services at the same time. This will in turn lead to more secure e-government services and eventually to building citizens' and stakeholders' trust in

adopting and using e-government services. However, it is important for organisations to cost-effectively manage security risks associated to e-government services, meaning that before implementing security solutions – cost benefit analyses should be conducted and weighted between the values of what is to be protected and what security measures need to be implemented.

Further research work will include developing a secured e-government maturity model (SeGMM) which will be the result of integrating the ISMM proposed in this paper into an e-government maturity model (eGMM) (Karokola et al, 2010b). The new model is expected to guide and benchmark effectively secure e-government services.

7. References

Anderson, P.W. (2001), "Information security governance" - information security technical report, volume 6, Number 3, pp. 60 – 70, (Available at http://www.sciencedirect.com/science/article/pii/S1363412701003090, Last accessed on March, 2011).

Bishop, M. (2006), "Computer Security" – Arts and Science – Addison-Wesley, ISBN: 978-0-201-44099-7.

CC. (2009)":The Common Criteria - PART1V3.1R3", (Available at http://www.commoncriteriaportal.org/, Last accessed February, 2011).

Chiang, T., Chang, R., Kouh, J., & Hsu, K. (2008), "An information Security Education Maturity Model", (Available at http://cnte2008.cs.nhcue.edu.tw/pdf/135.pdf, last accessed March 2011).

CitiGroup. (2000), "Secretary of defense Corporate fellows program", Final report, (available at http://www.ndu.edu/sdcfp/reports/Citigroup.doc, last accessed January, 2011)

Dhillon, G. (2000), "Challenges in managing Information Security in the millennium", Idea Group Publisher pp. 1-8, ISBN: 978-1-87828-978-0

Dzazali, S., Sulaiman, A., & Zolait, A. (2009), "Information Security Landscape and Maturity Level: Case Study of Malaysian Public Service (MPS) Organizations"; Government Information Quarterly 26 (2009) pp. 584-593, (Available at http://www.sciencedirect.com/science/article/pii/S0740624X09000859, Last accessed on March, 2011).

Fraunhofer (2002), "Security Maturity Model (SMM)", Institut Software und Systemtechnik, Germany, (Also available at http://www.isst.fraunhofer.de/Images/Jahresbericht_2002_tcm81-23346.pdf, last accessed March, 2011)

Henry, K. (2004), "The human side of information security" – information security handbook, 5th edition Boca Raton, London, New York, Washington, DC.

IBM-ISF. (2007), "Introducing the IBM security Framework and IBM Security Blueprint to Realize Business" - Driven Security Red guides for Business Leaders, (Also available at http://www.redbooks.ibm.com/redpieces/pdfs/redp4528.pdf, Last accessed March, 2011).

ISM3 Consortium. (2007), "Information Security Management Maturity Model version 2.10" Consortium, (Also available at http://www.ism3.com/, Last access September, 2010).

ISO-27K, (2008), "ISO/IEC 27005:2008, Information technology -- Security techniques -- Information security risk management"

Kaminski, K. (1999), "In defense of the naïve Inductivist: As Well as some of their Not-so-Naïve Brethren" (Available at http://www.springerlink.com/content/l65154n79754q562/fulltext.pdf, last accessed March, 2011).

Karokola, G. (2010a), "A Systemic Analysis of e-Government Maturity Models: The Need For Security Services - A Case of Developing Regions" Licentiate of Philosophy Thesis, Department of Computer and Systems Sciences, University of Stockholm/Royal Institute of Technology, Stockholm ISSN: 1101-8526.

Karokola, G. & Yngström, L. (2009a), "Discussing e-Government Maturity Models for the Developing World – Security View". Proceedings of the 8th ISSA conference on Information Security, University of Johannesburg, Johannesburg, South Africa, pp. 81-98, ISBN: 978-1-86854-740-1,

Karokola, G. & Yngström, L. 2009b), "State of e-Government Development in the Developing World: Case of Tanzania – Security View" Proceedings of the ICEG - 5th International Conference on e-Government. Suffolk University, Boston, USA. 19 – 20 October, 2009. ISBN: 978-1-906638-49-8,

Karokola, G., Yngström, L., & Kowalski, S. (2010b), "A Comparative Analysis of e-Government Maturity Models for Developing Regions: The Need for Security Services". Unpublished paper – submitted to the International Journal of Electronic Government Research (IJEGR) - IGI,

Kowalski, S. (1994), "IT Insecurity: A Multi-disciplinary Inquiry", PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and Royal Institute of Technology, Stockholm ISBN: 91-7153-207-2.

Lessing, M.M. (2008), "Best practices show the way to information Security maturity", (Available at http://researchspace.csir.co.za/dspace/handle/10204/3156, last accessed March, 2011).

Martins, A & Eloff, J. (2002), "Information security culture", IFIP TC11, 17th international conference on information security (SEC2002) Cairo, Egypt.

McGraw, G. (2005), "Software Security" Addison-Wesley software security series, ISBN: 978-0-321-35670-3.

Neubauer, T. , Klemen, M., and Biffl, S. (2005), "Business Process-Based Valuation of IT Security" (Also available at http://uqu.edu.sa/files2/tiny_mce/plugins/filemanager/files/4150111/bpr/20-pub-inf_3354.pdf, last accessed March, 2011).

NIST (IR7358), (2007), "Program Review for Information Security Management Assistance" – PRISMA, (Available at http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf, last accessed March, 2011).

NIST (SP800-30), (2002), "Risk Management Guide for Information Technology Systems", (Available at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, last accessed March, 2011).

Rao, V & Jamieson, R. (2003), "An Approach to Implementing Maturity Models in IT Security", Proceedings of the 14th Australasian conference on information systems (Available at http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1305&context=acis2003, Last accessed March, 2011).

Siponen, T.M. (2003), "Information security management standards: Problem and solutions", proceedings of the 7th Pacific Asia Conference on information systems, pp. 1550 – 1561, (Available at http://www.pacis-net.org/file/2003/papers/security/284.pdf, Last accessed March, 2011).

SSE-CMM. (2003), "Systems Security Engineering Capability maturity Models (SSE-CMM) ver. 3", (Available at http://www.sse-cmm.org/docs/ssecmmv3final.pdf, last accessed March, 2011).

TZ-TCRA, Tanzania Communication Regulatory Authority (2010): (Available at http://www.tcra.go.tz, last access 15th of February, 2010).

Thomson, K. & Solms, R. (2006), "Towards an Information Security Competence Maturity Model" (Available at linkinghub.elsevier.com/retrieve/pii/S1361372306703566, last accessed February, 2011).

Walsh, D., & Downe, S. (2005), "Meta-synthesis method for qualitative research: A literature review" (Available at http://onlinelibrary.wiley.com/doi/10.1111/j.1365-2648.2005.03380.x/pdf, March, 2011).

Kothali, C. R. (2004), "Research Methodology: Methods and techniques, 2nd ed. New Age Publication, New Delhi".

Wimmer, M & Bredow, B. (2001), "e-Government: Aspect of Security on different layers" (Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=953086, last accessed March, 2011).

Woodhouse, S. (2008a), "An ISMS (Im) – Maturity Capability Model", Proceedings of the IEEE 8th International Conference on Computer and Information Technology Workshops, (Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber =4568510, Last accessed March, 2011).

Woodhouse, S. (2008b), "Information Security: End User Behavior and Corporate Culture", Proceedings of the IEEE 7th International Conference on Computer and Information Technology, (Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp =&arnumber=4385178, Last accessed March, 2011).

WorldBank. (2001), "e-Government and the World Bank" Issue Note (Available at http://www.worldbank.org/reference/, Last accessed, April, 2010)

Yngström, L. (1996), "A Systemic-Holistic Approach to Academic Programmes in IT Security", PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm and the Royal Institute of Technology, Stockholm; ISBN: 91-7153-521-7.