Routledge
Taylor & Francis Group

TECHNOLOGICAL AND ECONOMIC DEVELOPMENT OF ECONOMY
ISSN 2029-4913 print/ISSN 2029-4921 online

2012 Volume 18(1): 117–131
doi:10.3846/20294913.2012.661196

A SUSTAINABLE INFORMATION SECURITY FRAMEWORK FOR E-GOVERNMENT – CASE OF TANZANIA

Carina Kabajunga Wangwe[1], Maria Margaretha Eloff[2], Lucas Venter[3]

[1, 2]University of South Africa, P O Box 392 UNISA 000, South Africa
[3]North West University, Private Bag X1290, Potchefstroom 2520, South Africa
E-mails: [1]arina.wangwe@gmail.com (corresponding author); [2]eloffmm@unisa.ac.za; [3]lucas.venter@nwu.ac.za

Received 21 September 2010; accepted 05 November 2011

Abstract. The government of Tanzania adopted an e-Government strategy in 2009 that is aimed at improving efficiency in government and providing better services to citizens. Information security is identified as one of the requirements for the successful e-Government implementation although the government has not adopted any standards or issued guidelines to government agencies with regards to information security. Comprehensive addressing of information security can be an expensive undertaking and without guidelines information security implementations may be more prone to failure. In a resource poor country such as Tanzania, there is a need for a cost effective and sustainable means of addressing information security in e-Government implementations. In this paper the authors present a case study of an e-Government interaction between a ministry and a government agency and the information security challenges identified in the implementation. In order to address these challenges an information security framework is conceptualized using action research. The framework is applied in the case study to address the identified challenges and the means to address future challenges in a sustainable manner is identified. Finally, the proposed framework is evaluated against Tanzanian and international metrics.

Keywords: information security framework, e-Government, information security, e-Governance, e-Government in Tanzania.

Reference to this paper should be made as follows: Wangwe, C. K.; Eloff, M. M.; Venter, L. 2012. A sustainable information security framework for e-Government – case of Tanzania, *Technological and Economic Development of Economy* 18(1): 117–131.

JEL Classification: O14, O33, O38.

1. Introduction

Tanzania is a country in East Africa with a population of about 43 million people and per capita GDP in 2009 of Tanzania Shillings 693.185 or USD 522 (Ministry of Finance and Economic Affairs 2010a). The government of Tanzania consists of central government ministries, departments and government agencies or parastatal organizations. These are commonly referred to by the acronym MDAs. Tanzania has recognized information and communication technologies as a tool for development of the country. There is a national ICT Policy (Ministry of Communications and Transport 2003) that was adopted in 2003 with the intention to guide national ICT initiatives. However, each ministry within central government and each municipality within local government set their own agenda in relation to ICT. The central government budget for the financial year 2010/2011 by the Ministry of Communication, Science & Technology which is responsible for ICT was Tanzania Shillings 3.1 billion which is equivalent to about USD 2 Million (Ministry of Finance and Economic Affairs 2010b). Despite its low GDP and low ICT spending, mobile phone penetration in Tanzania is fairly high, standing at 31% of the population, and the private sector has introduced many services to take advantage of the high use of mobile phones (Hellström 2010: 14). Citizens expect government to keep up with these innovations and in response the government of Tanzania has come up with policies and strategies to harness the use of ICT including an e-Government strategy.

This Tanzanian e-Government strategy (President's Office United Republic of Tanzania 2009) is aimed at improving efficiency in government and providing better services to citizens. The strategy outlines seven guiding principles including: Service Innovation; Equal Access; Ease of Use; Benefit Realization and Involvement of All Stakeholders; Security and Privacy; Partnership and Outsourcing; and Interoperability. The two principles that relate directly to information security are *Security and Privacy* and *Interoperability*. The strategy lists six critical success factors, one of which is sustainable infrastructure, and goes further to state one of the requirements of a sustainable infrastructure as being network and information security. However, the strategy does not provide guidance to MDAs, who are the major implementers of e-Government, on how to go about addressing information security issues. Furthermore, there are no other government-wide policies, guidelines or standards that have been issued with regards to information security. In order for citizens to benefit from e-Government, MDAs must collaborate and cooperate to come with comprehensive services that are efficient and secure.

Implementation of robust information security can be an expensive undertaking. Since Tanzania is a country with limited resources, it is important for MDAs to have a framework which allows them to plan for and implement information security in e-Government implementations, but at the same is cognizant of the limited resources that are at the MDAs disposal. This paper presents such a framework and uses a case study of an e-Government implementation in Tanzania to illustrate how the framework can be applied.

This paper aims at answering the research question "How can a cost effective and sustainable information security framework for e-Government be developed for Tanzanian MDAs?". Action research is used as the methodology for a case study involving an e-Government transaction between a government ministry and a government agency. The observations resulting from the study are combined with secondary data from the literature review resulting in an information security framework that answers the research question.

The remainder of this paper is structured as follows: section 2 presents the case study of a Government to Government implementation and the approach to solve the identified information security challenges. Section 3 discusses literature that is relevant to the study that is used to gain insights on how to solve the identified challenges. In section 4 a conceptual framework is proposed and then applied to the case study. Section 5 presents an evaluation of the frameworks using Critical Success Factors. The paper ends with a conclusion in section 6.

2. Case study

2.1. Background

The Tanzanian Central Government has been paying pensions for civil servants who retired before July 2004 through a ministry responsible for finance. Due to concerns about the efficiency of the process, fraud and resource constraints, the ministry decided to outsource the process in 2008 to a government agency. The government agency chosen is one that has been dealing with pension payments for over 30 years for employees from the private sector and from other government agencies. The ministry required the government agency to run the payroll on secure software and send the payroll information electronically to banks. The banks would then debit the ministry account and credit the pensioners account. The ministry envisaged that this process would reduce human intervention which is one of the sources of fraud; ensure that pensioners are paid on time; and have an audit trail of transactions so as to follow up on any suspect cases. Furthermore, by outsourcing the arrangement to an agency that already had a robust software, and business continuity program in place, the risks arising from frequent power interruptions and lack of sufficient technical skills in the ministry would be addressed.

2.2. Challenges identified in implementing the decision

The process of implementing the decision began with a kickoff workshop involving staff from the ministry and the agency. Several challenges were identified during the workshop and when the action plan for implementation was started. These challenges are categorized in three pillars. For ease of reference the challenges are given code numbers. These are:

a) **Governance**
  - G1: Legally, the agency had no mandate to access the data held by the ministry or to pay pensions on behalf of the ministry.
  - G2: Both ministry and agency had information security policies that needed to be aligned for purposes of the transaction.
  - G3: The memorandum of understanding (MoU) signed between the Ministry and the agency did not explicitly address information security.

b) **Operational**
  - O1: Definitions of some terms were different. For example a survivor's pension in the central government ministry is different from a survivor's pension in the government agency.
  - O2: Financial resources allocated to the outsourcing project were limited.

- O3: The ministry wanted to retain some control over updates to information
- O4: Technical and management teams met separately during the planning process.
- O5: The organizational culture for the two organizations was found to be different. In the agency technical staff spearhead most initiatives and sold ideas to management, while in the ministry the approach was more top down, that is directives are given by the minister, which the technical and operational staff have to implement.

c) **Technical**

- T1: Some of the necessary data was mostly in paper files and confidentiality and privacy was observed through physical access controls such as storing the data in locked cabinets. Access lists were on paper and files containing information were issued by a person responsible for storing the files.
- T2: The ministry was running their payroll on a COBOL based application while the government agency was using an application based on Oracle Forms. The underlying databases and operating systems were also on different platforms.
- T3: The ministry offices and the agency offices had no direct data communication link.
- T4: Although security policies existed in both organizations, no standard requirements for security were set out in either policy.

The initial approach by the Ministry was to deal with the issue of legislation, and propose amendments to the law which were passed by the Parliament (Parliament of Tanzania 2008). These amendments simply allowed the agency to pay pensions on behalf of the government. The challenge of data access was not addressed. A technical team headed by one of the authors of this paper, was set up by the agency to coordinate the project implementation. This team decided to adopt a structured approach to address the challenges mentioned above. The process which is an ongoing iterative process uses the action research methodology (de Villiers 2005) as shown in Figure 1.

Early in the process, the authors observed that some of the challenges identified have been addressed by studies already published in journals or conferences proceedings. The reuse of solutions or components of the solutions presented in such studies could be beneficial to the case study. This resulted in literature surveys that identified some relevant studies. These studies are outlined in the next section and how they meet the challenges identified is discussed.

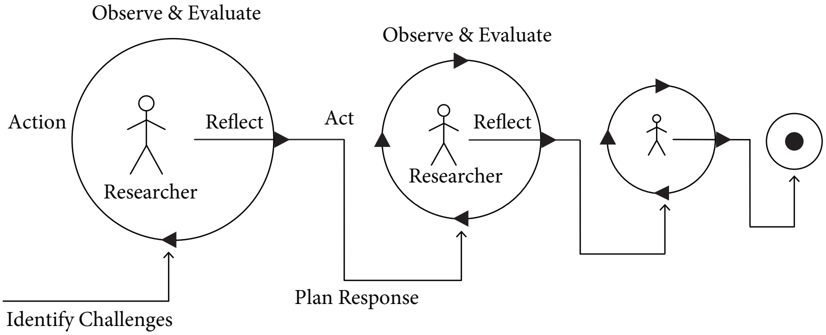

Fig. 1. Action research process: adopted from de Villiers (2005)

3. Literature survey

The starting point for the literature survey was existing international standards on information security. The International Organization for Standardization (ISO) defines information security as the preservation of confidentiality, integrity and may also involve authenticity, accountability, non-repudiation and reliability (ISO/IEC 2009: 3). Information security has been studied comprehensively from a technical and a management perspective. A few studies have also been done on information security in Tanzania. In this section, studies related to information security in e-Government are discussed in relation to the challenges observed in the case study. The studies are presented in three categories, which are, technical, management and studies based in Tanzania.

3.1. Technical studies on information security in e-Government

Many e-Government implementations are achieved through Service Oriented Architectures (SOA) with Web Services (Chunnian *et al.* 2011; Simon *et al.* 2010; Scholl, Pardo 2010). This is because e-Government implementations involve transactions across heterogeneous systems.

The security requirements for e-Government implementations are discussed by Zissis and Lekkas (2011) in fiver broad categories which are Availability, Confidentiality, Integrity, Authenticity, and Accountability. The security requirements of a particular e-Government project, the Access e-Gov project (Durbeck *et al.* 2007) are listed as Communication security that can be achieved through standards-based encryption and digital signatures; Trust; Privacy; and access control: whereby Attribute Based Access Control is suggested to provide a flexible dynamic infrastructure that suits loosely coupled SOA. Beimel and Peleg (2011) introduce an improved method of Access Control policy composition which underpins access control with ontologies through the application of the Web Ontology Language (OWL) and the Semantic Web Rule Language (SWRL).

The use of the Security Assertion Mark-up Language (SAML) as a mechanism for handling access control in an e-Government transaction was addressed in a study by Marin-Lopez *et al.* (2011) and by Wangwe *et al.* (2008). SAML is one of several open technical standards adopted by the Organization for the Advancement of Structured Information Standards (OASIS). Other standards from OASIS include XACML which is designed for access control and the WS family of standards for web service security (OASIS 2010).

3.2. Information security management

ISO 27002, which is an internationally accepted standard, requires legal and regulatory aspects to be taken into consideration when incorporating security requirements in the design of systems (ISO/IEC 2005). To this end, Guarda and Zannone (2009) state that legal requirements should be incorporated into software engineering for e-Government transactions by following existing laws and more especially those related to privacy and data protection. A practical implementation of how legal requirements can be incorporated in software system engineering is demonstrated in a study by Islam *et al.* (2011) in a framework that allows developers to elicit requirements from legislation, and track that these requirements are addressed through the system development.

A study by Seidenspinner and Theuner (2007) investigates different cultural environments and concludes that the cultural environment of users affects their online behaviour. This conclusion is extended to governments in a proposition by Alfawaz *et al.* (2008) that national culture may have an impact on e-Government security effectiveness in developing countries. Their study looks at the effect of legislation on security and privacy and states that many developing countries have yet to consider adopting adequate legislation related to information security management which could be used to take action against the misuse of ICT resources. Zarei and Ghapanchi (2008), however, argue that e-Government development should not wait until full security levels are reached. They state that providing fully functional security for all the e-Government programs is impractical. Other security heuristic principles include the need for a security development and management plan and application of security standards by a team with sufficient experience. The recommendations of the study by Zarei and Ghapanchi are to an extent validated by a study conducted in South Africa by Dagada *et al.* (2009) who conclude that while legislation that deals with information security exists, it is not used in organizational policies.

Several governments have put in place mechanisms at a national level to govern information security. For instance, the government of the United Kingdom adopted Her Majesty's Government (HMG) Security Policy Framework that sets out policy areas to guide information security management in government departments (Cabinet Office UK 2008). The Government of Tasmania has adopted an Information Security Framework which provides guidance to government agencies on what Information Security Policy Principles they need to adhere to, as well as important legislative requirements and the primary roles and responsibilities for information security (Department of Premier and Government, Tasmania 2009). A slightly different approach has been adopted by the Spanish and South African Governments, who have adopted interoperability standards for government agencies that address security among other issues (Ministry of the Presidency, Spain 2010; SITA 2007).

3.3. Information security and e-Government in Tanzania

In Tanzania, a study of information security in higher institutions of learning (Bakari *et al.* 2005) led to two key conclusions, which were, the necessity of adequate planning at national and organizational level for a successful information strategy; and the need for developing countries to transform traditional information security policies into relevant policies to cater for digital information security. These conclusions further motivate this study since a framework for e-Government security would both ease planning at a national and organizational level, and also guide the drafting of relevant security policies.

The need for regulations to underpin information security is discussed by Tarimo (Tarimo *et al.* 2005) who recognizes contexts in developing countries as significantly different from those in developed countries, and the impact on information security. Tarimo *et al.* conclude that instead of waiting for the government intervention, organisations deploying ICT can put forward their own initiatives to make sure that their systems follow standards that allow for security, interconnectivity and interoperability with other ICTs in the country and beyond. This conclusion is supported by the study Zarei and Ghapanchi (2008), which is to say that for a developing country; a top-down might not work since governments are slow in implementing the necessary governance structure, while a bottom- up approach may be constrained by lack of guidelines.

Karokola (Karokola, Yngstrom 2009) study Tanzanian government institutions' requirements with regards to information security and come up with a score of the priority areas. Technical security issues are ranked most important together with awareness. Non-technical aspects including managerial, operational and economical factors are also considered priority areas. This study shows that legal and regulatory requirements are not high on the list of priorities. This could be explained by the fact that there are currently not many laws in Tanzania that address information security.

3.4. Reflection on the literature survey

The literature survey provided useful insights to addressing the information security challenges that were identified in the case study, and in particular in highlighting areas where solutions to similar challenges have already been found and how other governments have approached information security management. The insights to some of the challenges obtained from the literature survey are summarised in Table 1. For challenges, G2, O2, O4 and T3 which are very specific to the case study, ways to address the challenges were obtained through brainstorming sessions, and the findings incorporated in the framework that is presented in section 4.

Table 1. Insights from literature surveyed

Identified Challenges	Insights from studies surveyed
Governance	
G1	Where legislation exists, it should be reflected in policies. International Standards should be used to guide implementations
G3	Technical and operational solutions can and should be used in the absence of governance structures
Operational	
O1	Semantic interoperability can be achieved through common taxonomies
O3	Robust Access control mechanisms are important for secure government to government transactions. Attribute Based Access Control is a mechanism that can be used with SOA to ensure controlled access to information assets
O5	Culture has an impact on web usage in general, and specifically on information security for online transactions. The implementation of successful information security implementations should thus include addressing of culture
Technical	
T1	Access control lists can be translated into electronic polices using open standards such as XACML and implemented using SAML
T2	Service Oriented Architectures and Web Services can be used for technical interoperability; in addition semantic interoperability can be achieved through use of ontologies
T4	In general, Security Objectives are Confidentiality which includes authentication, authorization and access control and privacy, Integrity, Availability and Accountability which includes Trust and Non repudiation

4. Proposed framework

The insights obtained from the literature survey were combined with data collected through observations of current information security practices in both the ministry and the agency, and interviews with staff involved in the implementation of the case study. From these, the authors conceptualized an information security framework that is referred to by the acronym TOG (Technical, Operational and Governance). The TOG framework recognizes the need for e-government transactions to be cognizant of national legislation, and policies, will at the same time complying with organizational policies. At the technical level, for a country that has limited resources such as Tanzania, the technical pillar recognizes the existence of tried and test mechanisms, particularly those based on open internationally accepted standards.

The TOG information security framework consists of three pillars which are Technical, Operational and Governance pillars. The governance pillar includes legislation, internationally acceptable standards, national and regional standards and guidelines and operational policies. This pillar will be typically implemented at national level by inter-ministerial committees together with legislative bodies such as parliament, while at MDA level it will be implemented by executive management and or Boards of Directors. The operational pillar includes organizational plans and operational procedure and is implemented by organizational units within MDAs. The technical pillar includes technical mechanisms to address the security requirements and is implemented by Information Technology departments within MDAs. The components of each pillar are gleaned from the literature study done of researches on information security for e-government and matched to security objectives and requirements that are applicable to the e-government transaction.The detailed TOG framework is depicted in Table 2.

Table 2. 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

4.1. Application of the framework

The application of the framework was done by the ministry and the agency with activities often taking place in parallel, and with the top management being responsible for governance, operational staff for the operational pillar and technical staff for the technical pillar. Mapping across the pillars was undertaken in workshops where management and technical staff met to discuss their activities and map them against activities being done in other pillars. This approach was termed a 'plug and play' approach in contrast to a top-down or bottom up approach, although for each activity a Plan-Do-Act-Check cycle was followed as shown in Figure 2. The plug and play approach recognises that resources in the Tanzania government for one big initiative may not be available, but it is still possible for a department to start to address information security for an e-government transaction by focusing first on one pillar of the framework – depending on what the role of the department is, and what resources are available. A mapping onto the other pillars can be done from time to time, as resources become available. Each mapping recognises the initiative already in place and gradually the government moves towards a holistic addressing of information security requirements.

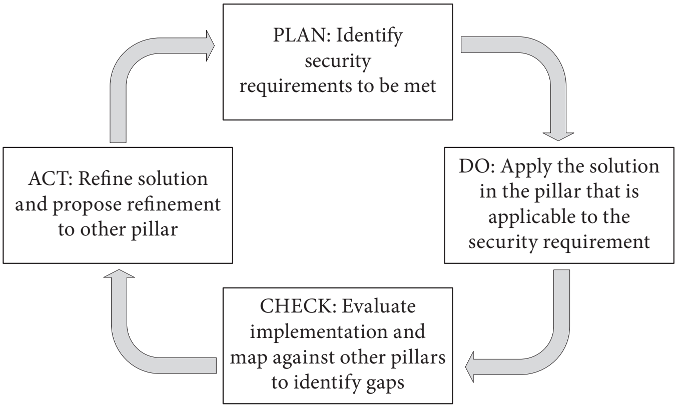
PLAN: Identify security requirements to be met
DO: Apply the solution in the pillar that is applicable to the security requirement
CHECK: Evaluate implementation and map against other pillars to identify gaps
ACT: Refine solution and propose refinement to other pillar

Fig. 2. PDCA Cycle for application of the TOG framework

The specific activities carried out so far in implementing the framework and addressing the challenges stated in section 2.2 are:

a) **Governance**

Legislation (Parliament of Tanzania 2008) was put in place to mandate the agency to pay on behalf of the ministry before the implementation of the framework. Based on the amended legislation a contract signed between the two parties to outline the roles and responsibilities of each party in implementing the outsourcing of payment of pensions. Furthermore the parties agree that the information security policy of the ministry would prevail.

b) **Operational**

In meeting the information security objectives, the following activities have been done:

- Risk assessment has been carried out and an access control list setup.
- The parties have agreed to use the Ministry definitions where terminology differs.

– Joint awareness sessions between technical and management teams are held every six months to review activities in each team and determine where solutions need to be mapped to each other.

Challenges that are still to be addressed include coming up with taxonomy of terms that relate to the payment of pensions to ensure that interpretation of the terms is consistent.

c) **Technical**

The technical team has developed a payroll web service that can be invoked by the ministry if they need to do updates to data. The same web service is used to run the payroll. In addressing data integrity, privacy and confidentiality, a secure communication link has been set up between the ministry and the agency and information across the link is encrypted. The relevant information security policies translated to XACML. Authentication has been tied to fixed IP addresses. Availability has been addressed through the installation of UPS for power management. The agency uses an SSL certificate issued by VeriSign (www.verisign.com) for its browser interfaces. Thus VeriSign was used as a trusted third party in the absence of a certificate authority set up by government. The challenges that still need to be addressed include automating the issue of security assertions, by for example, implementing SAML. Table 3 illustrates how the TOG framework has been applied.

Table 3. Application of TOG framework to payroll application

		PILLAR		
Security Objective	**Security Requirement**	**Governance**	**Operational**	**Technical**
Confidentiality	Authentication	• Ministry's Information Security Policy		
	Authorization and Access Control	• Finance Act. No. 13 of 2008 • Contract between Ministry and Agency	• Risk Assessment, Access Control List, • Standard Terminology for transactions • Awareness Sessions	• XACML policies based on Ministry's information Security Policy
	Privacy	• Ministry's Information Security Policy		
Integrity	Data Integrity	• Ministry's Information Security Policy		• SSL, Encryption
Availability	Availability			• Uninterruptible Power Supply (UPS); • Pensioner Payroll Web Service
Accountability	Trust & Non Repudiation	• Finance Act No. 13 of 2008 • Contract between Ministry and Agency	• Access Control List	• SSL (from VeriSign) • Authentication by IP address

4.2. Addressing future challenges

The TOG framework allows MDAs to include any technical, operational or governance solutions or practices that are applicable in the context of the transactions being addressed. Once a solution has been adopted in one pillar, mapping will be done across the other pillars to ensure that comprehensive information security is achieved.

5. Evaluation

The TOG framework is evaluated using critical success factors (CSFs). The evaluation is shown in Table 3. CSFs have been used as a method for helping organizations guide the development and management of security strategies and across their enterprises and for evaluation of information systems (Caralli 2004) (Bergeron, Bégin 1989). The TOG framework is evaluated in two ways. Firstly Critical Success Factors (CSFs) stated in the Tanzania e-Government strategy are used. Although the CSFs are stated in relation to e-Government they can also be applied to information security in e-Government since information security should form an integral part of the planning process for e-Government implementations conception to conclusion. Secondly, CSFs stated in the ISO 27002 information security management standard are used. This is done in order to determine how the TOG framework measures up against an international standard. ISMS Critical Success Factors have been adopted by ISO in the ISO/IEC Code of practice of information security management (ISO/IEC 2005: 11). These are applicable to the evaluation of TOG since TOG is designed to address management aspects of information security.

The evaluation of the TOG framework against the Tanzania e-Government Strategy and the ISO ISMS CSFs are presented in Table 4 and Table 5 respectively.

Table 4. Evaluation of TOG against Tanzania e-Government Strategy CSFs

CRITICAL SUCCESS FACTOR	TOG Solution
Political will, support and commitment	All legislation in Tanzania is passed through the parliament. The Governance pillar of TOG which includes legislation enables political leaders to understand the role they need to play to have successful information security in e-Government implementation
Availability of HR capacity	TOG addresses HR capacity by its flexible structure that refers to international open standards. So, there is no need for MDAs to reinvent the wheel where proven standards are already in place. In addition, the PDCA implementation process helps the existing HR resources to continually check where gaps in implementation are and focus the upgrading of skills or looking for new resources on the areas where skills are lacking
Institutional and Legal framework	The TOG governance pillar includes all relevant legislation and organizational policies that address how a security requirement is to be met. These are then mapped onto organizational plans and procedures in the operational pillar
Financial resources	TOG is a flexible framework whose 'plug and play' of 'start anywhere' nature means that the technical, operational and governance components to address each security requirement can be implemented as and when resources are available within the identified risks acceptance level

End of Table 4

CRITICAL SUCCESS FACTOR	TOG Solution
Commitment by all actors	Implementation of the TOG framework forces the involvement and collaboration of technical operational and management staff. Every technical implementation needs to be mapped back onto an operational procedure and or governance structure and vice versa
Sustainable infrastructure	The technical pillar emphasizes the use of open standards, and service oriented architectures which address the lack of interoperability that may exist among MDAs. In addition the 'start anywhere' and flexible approach to implementing TOG means that each MDA can start with addressing the requirements in a manner that takes the context of the implementation into consideration, then build upon that implementation as resources improve, or review and change the implementation if necessary

Table 5. Evaluation of TOG against ISMS CSFs

ISMS CRITICAL SUCCESS FACTORS	TOG Solution
Information security policy, objectives and activities aligned with objectives	TOG addresses information security policies and provides for the mapping of those policies to operational and technical activities
An approach and framework for designing, implementing, monitoring, maintaining and improving information security consistent with the organizational culture	The TOG framework allows for organizational culture especially in the context of Tanzania where it is often not possible to have a strictly hierarchical or sequential process. TOG allow for various start points in any of the pillars and then subsequent mapping to any of the other pillars, provided that the security objectives are set in advance
Visible support and commitment from all levels of management especially top management	Implementation of the TOG framework forces the involvement of technical operational and management staff
An understanding of information asset protections achieved through the application of information security risk management	Risk Assessment is provided for in the operational pillar of TOG
An effective information security awareness, training and education program information all employees and other relevant parties of their information security obligations set forth in the information security policies, standards etc., and motivate them to act accordingly	Awareness is provided for in the operational pillar of TOG
An effective information security incident management process	TOG does not address this. Such a process, however, can be included in the Operational Pillar
An effective business continuity management approach	Business continuity management is provided for in the TOG framework in order to address the Availability security objective
A measurement systems used to evaluate performance in information security management and feedback suggestions for improvement	The PDCA cycle approach can be used to implement TOG

The evaluation of the TOG framework shows that it is a robust framework since it addressed most of the factors in an internationally accepted standard, which is ISO/IEC 27002. At the same, it is a sustainable framework for Tanzania as it addresses all the critical success factors stated in the Tanzanian e-Government strategy.

6. Conclusion and further work

This paper aimed to answer the research question "How can a cost effective and sustainable information security framework for e-Government be developed for Tanzanian MDAs?". To answer the question, a framework that identifies security objectives and requirements has been presented. The framework, dubbed the TOG framework, consists of three pillars, namely governance, operational and technical. Together these pillars allow an MDA to address information security comprehensively while at the same time allow flexibility in the implementation to cater for resource and other constraints. The framework is sustainable in that it proposes the use of open standards and service oriented architectures while meeting any legal or regulatory requirements. TOG also allows a 'plug and play' approach so that MDAs can start with a solution in any of the pillars for which resources are available and then move towards a comprehensive solution by mapping solutions from one pillar to another. The framework has been successfully applied to a case study. The evaluation of the framework shows that TOG addresses all the CSFs stated in Tanzania's e-Government strategy while meeting all except one of the CSFs proposed by the ISO in its information security management system standard. This evaluation leads to the conclusion that the proposed framework is a robust, sustainable and cost effective framework that is applicable to MDAs in Tanzania. The proposed framework adds to the body of knowledge in the field of information security as it shows how the Tanzania context of e-Government transactions can be addressed. While the mechanisms presented within the framework are tried and tested, the framework shows how these can be combined, as and when resources allow, going towards a holistic addressing of the information security. This is the innovation of this approach rather than the government adopting without modification either a standard or copying another countries' framework. At the same time the framework enables different levels in government to address the same requirements through different mechanism depending on their areas of expertise and then provides a means for the others to map these onto their initiatives.

The authors intend to extend the study to determine whether the framework would be applicable in the East African Community, as the countries in the EAC have similar challenges in terms of information security as those in Tanzania.

References

Alfawaz, S.; May, L.; Mohanak, K. 2008. E-government security in developing countries: a managerial conceptual framework, in *International Research Society for Public Management Conference,* 26–28 March 2008. Queensland University of Technology, Brisbane.

Bakari, J. K.; Tarimo, C. N.; Ynstrom, L.; Magnusson, C. 2005. *State of ICT Security Management in the Institutions of Higher Learning in Developing Countries*: Tanzania Case Study. ICALT, 1007–1011.

Beimel, D.; Peleg, M. 2011. Using OWL and SWRL to represent and reason with situation-based access control policies, *Data & Knowledge Engineering* 70(6): 596–615. http://dx.doi.org/10.1016/j.datak.2011.03.006

Bergeron, F.; Bégin, C. 1989. The use of critical success factors in evaluation of information systems, *Journal of Management Information Systems*: 111–124.

Cabinet Office UK. 2008. HMG Security Policy Framework. Available from Internet: http://www.cabinetoffice.gov.uk/media/111428/spf.pdf

Caralli, R. A. 2004. *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management*. Software Engineering Institute - Carnegie Mellon, Pittsburgh.

Chunnian, L.; Yiyun, H.; Qin, P. 2011. A Study on technology architecture and serving approaches of electronic Government system, *Intelligent Computing and Information Science, Communications in Computer and Information Science* 134(1): 112–117.

Dagada, R.; Eloff, M. M.; Venter, L. M. 2009. *Too Many Laws But Very Little Progress - Is South African Highly Acclaimed Information Security Legislation Redundant*? Informaton Security South Africa (ISSA09).

de Villiers, M. 2005. *Three Approaches as Pillars for Interpretive Information Systems Research: Development Research, Action Research and Grounded Theory*. SAICSIT, 142–151.

Department of Premier and Government, Tasmania. 2009. Tasmanian Government Information Security Framework.

Durbeck, S.; Schillinger, R.; Kolter, J. 2007. Security Requirements for a Semantic Service-oriented Architecture, in *The Second International Conference on Availability, Reliability and Security*, 366–373. IEEE Computer Society.

Guarda, P.; Zannone, N. 2009. Towards the development of privacy-aware systems, *Information and Software Technology* 51(2): 337–350. http://dx.doi.org/10.1016/j.infsof.2008.04.004

Hellström, J. 2010. *The innovative use of mobile applications in East Africa*. SIDA.

Islam, S.; Mouratidis, H.; Jurjens, J. 2011. A framework to support alignment of secure software engineering with legal regulations, *Software and Systems Modeling* 10(3): 369–397. http://dx.doi.org/10.1007/s10270-010-0154-z

ISO/IEC. 2005. ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management.

ISO/IEC. 2009. Information technology - Security techniques - Information security management systems - Overview and vocabulary.

Karokola, G.; Yngstrom, L. 2009. *Discussing e-Government Maturity Models for Developing World - Security View*. Information Security South Africa (ISSA09).

Marin-Lopez, R.; Pereniguez, F.; Lopez, G.; Perez-Mendez, A. 2011. Providing EAP-based Kerberos pre-authentication and advanced authorization for network federations, *Computer Standards and Interfaces* 33(5): 494–504. http://dx.doi.org/10.1016/j.csi.2011.02.005

Ministry of Communications and Transport. 2003. National Information and Communications Technologies Policy. United Republic of Tanzania, Dar es Salaam.

Ministry of Finance and Economic Affairs. 2010a. Hali ya uchumi ya Taifa katika Mwaka 2009 Jedwali Na. A. [State of the Economy of the Nation in 2009, Document No. A].

Ministry of Finance and Economic Affairs. 2010b. Volume IV- Public expenditure Estimates, Development Votes for 2010/11.

Ministry of the Presidency, Spain. 2010. Spanish National Interoperability Framework.

OASIS. 2010. Available from Internet: http://www.oasis-open.org/specs/

Parliament of Tanzania. 2008. Finance Act No. 13.

President's Office United Republic of Tanzania. 2009. Tanzania e-Government Strategy.

Scholl, H. J.; Pardo, T. A. 2010. Data-Centric Workflows in Government: a New Avenue of Research?, in *11th Annual International Digital Government Research Conference*, 138–146.

Seidenspinner, M.; Theuner, G. 2007. Intercultural aspects of online communication a comparison of mandarin-speaking, US, Egyptian and German user preferences, *Journal of Business Economics and Management* 8(2): 101–109. http://dx.doi.org/10.1080/16111699.2007.9636157

Simon, B.; Laszlo, Z.; Goldschmidt, B.; Kondorosi, K.; Risztics, P. 2010. Evaluation of WS-* Standards Based Interoperability of SOA Products for the Hungarian e-Government Infrastructure, in *4th International Conference on Digital Society*, 118–123. http://dx.doi.org/10.1109/ICDS.2010.28

SITA. 2007. Minimum Interoperability Standards for Information Systems in Government. Available from Internet: http://www.sita.co.za/standard/MIOSv4.12007.pdf

Tarimo, C. N.; Yngstrom, L.; Kowalski, S. 2005. An Approach to Enhance ICT Infrastrcutures Security through Legal, Regulatory Influence, *ISSA*, 1–12.

Wangwe, C. K.; Eloff, M. M.; Venter, L. 2008. *A Proposed Implementation of SAML V2.0 in an e Government Setting*. IST Africa. Windhoek: IIMC International Information Management Corporation.

Zarei, B.; Ghapanchi, A. 2008. Guidelines for government-to-government initiative architecture in developing countries, *International Journal of Information Management* 28: 277–284. http://dx.doi.org/10.1016/j.ijinfomgt.2008.02.008

Zissis, D.; Lekkas, D. 2011. Securing e-Government and e-Voting with an open cloud computing architecture, *Government Information Quarterly* 28(2): 239–251. http://dx.doi.org/10.1016/j.giq.2010.05.010

Carina Kabajunga WANGWE is a Ph.D. student at University of South Africa (UNISA) and works for a government agency in Tanzania. Four articles that she wrote as the primary author have been published in peer reviewed conference proceedings.

Maria Margaretha ELOFF is a Professor at School of Computing UNISA who holds a Ph.D. from Rand Afrikaans University. She has published extensively in the field of information security.

Lucas VENTER is a Professor and Director: Research support at North Western University, and a Professor Extraordinaire at UNISA. He has published extensively on information security, mobile agents and curricula for computing.