Evaluating A Framework for Securing e-Government Services – A Case of Tanzania

Geoffrey Karokola
Stockholm University/DSV, Sweden
karokola@dsv.su.se

Stewart Kowalski
Gjøvik University College, Norway
stewart.kowalski@hig.no

Louise Yngström
Stockholm University/DSV, Sweden
louise@dsv.su.se

Abstract
The current and emerging security threats poses a variety of security risks to e-government services. The Tanzanian national e-government strategy recognizes the importance and use of e-government maturity models (eGMMs) as a tool for guiding and benchmarking e-government implementation and service delivery. However, the models lack security services (technical and non-technical) in their maturity stages – leading to misalignment of strategic objectives between e-government services and security services. To bridge the existing security services gap in eGMMs – a framework for securing e-government services which integrates IT security services into maturity stages of eGMMs was proposed. The goal of this paper is to present an outline of the evaluation results for the proposed framework, in the context of a developing world environment. In the process, seven evaluation criteria were developed; thereafter, a case-study was conducted into six government organizations located in Tanzania. The overall results show that the framework was accepted in the studied environment. The framework usefulness was perceived highest at 95%; the framework dynamics & flexibility was perceived lowest at 76%.

Keywords: e-Government, framework, security services, technical, non-technical, maturity model

1. Introduction

e-Government services have become one of the most important and efficient means by which governments can interact with citizens and businesses. e-Government refers to “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) to promote citizens’ empowerment, improve government efficiency and service delivery, strengthen accountability and increase transparency” [24].

To guide and benchmark e-government implementation international organizations, consulting firms, academia and individual researchers have proposed various types of e-government implementation models, which are generally referred to as e-government maturity models (eGMMs). These models outline different maturity stages that a government can follow in order to offer the best and most efficient e-government services. A maturity stage reflects the level of e-government maturity, the degree of technology complexity, the degree of systems sophistication, and the level of interaction with users [5, 17, 24]. It is broadly recognized that the advantage of having a stage-wise approach in eGMMs is to offer governments the ability to measure the progress of e-government implementation, giving them flexibility to develop and prioritize e-government-related projects and activities, and facilitating organizations to meet their e-government goals by ensuring that business and technological components are effectively aligned [5, 21, 24].

However, effectively aligned does not necessarily mean being secure. By moving to more e-government services sophistication, e-government mission-critical information assets and/or infrastructures are exposed to more and in some cases to new security risks and threats. Customarily, interactions within and between governments (G), businesses (B) and citizens (C) require physical visits to government offices or use of physical mail services that pose tradition and well known threat to paper based information assets. Electronic services create new security challenges to government, business and citizens [1, 16].

Information security is a quality issue that cuts across the entire organization. It requires involvement of employees at all levels: strategic, tactical and operational. Information security is driven by a set of objectives and it improves quality of the services offered [8]. It ensures confidentiality, integrity and availability of critical information being stored, processed, and transmitted between e-government domains [1, 5, 16, 23, 28]. Therefore, security is an essential tool for managing security risks and threats in e-government services. Enhancing security services in e-government services will foster secure e-government services and consequently create confidence and trust among e-government users, leading to the success of e-government initiatives [21, 23].

The Tanzanian national e-government strategy recognizes the importance and use of eGMMs for guiding and benchmarking e-government implementation and service delivery. It suggests the use of eGMM with maturity stages similar to those of Gartner’s model [10, 20]. However, the findings from a comparative analysis of eleven eGMMs show that the models lack security services (technical and non-technical) in their maturity stages [13]. As a result, security services are often not considered in the early stages, such as during the planning, development, implementation, service delivery and maintenance phases of e-government projects; leads to misalignment of strategic objectives between e-government services and security services. Security services should be considered at the early stages of e-government services [15, 26]. Having security services being part of eGMMs – would insure that security is integrated into the maturity models stages from the beginning and not an after thought when something goes wrong. [13].

Responding to these problems, a framework for securing e-government services which integrates IT security services into...
eGMMs was developed [11]. Description of the framework is given in section two of this paper.

Being part of on-going research work – the goal of this paper is to present an outline of the evaluation results of the proposed framework [11], in the context of a developing world environment, where Tanzanian government organisations are used as a case study.

The remainder of the paper is organized as follows: section two presents background to the previous work; and section three presents the framework evaluation process and methodology. Section four presents data collection, processing and analysis techniques; and section five presents the discussion of the research results. Conclusion and future research work is given in section six.

2. Previous Work

As a background, the Tanzanian national e-government strategy recognizes the importance and use of eGMMs for guiding and benchmarking e-government implementation and service delivery. It suggests the use of eGMM with maturity stages similar to those of Gartner’s model [13, 20]. However, the findings from a comparative analysis of eleven eGMMs show that they lack security services (technical and non-technical) in their maturity stages [13]. To bridge the identified security services gap in eGMMs, a framework for securing e-government services which integrates IT security services into eGMMs was developed. The framework is shown in figure 1, and its catalogue of security services requirements control areas (SRCAs) is given in Annex–2 [11].

The framework development process involved extensive analysis of internationally recognised and widely used eleven eGMMs for security services. The results show that security services (technical and non-technical) are lacking in eGMMs [13]. The selected eGMMs were then synthesized to form eGMM with five maturity stages as a common frame of reference for eGMMs. The maturity stages were: web-presence, interaction, transaction, transformation, and continuous improvement [13]:

Web-presence maturity stage: is the initial stage where communication is one way. Government disseminates information to the citizens via static websites. Information is accessible online – mostly basic and limited options to citizens, including reports and publications. Interaction maturity stage: is the advanced stage of maturity stage one. Government provides enhanced interactive websites services with more capabilities to Citizens. Available services include search engines, documents downloading, filling forms online, chat rooms, and emails. Transaction maturity stage: is the third stage, enhanced with more sophisticated technologies. Citizens (users) can conduct complete on-line transactions of values. Available services include taxes assessment and payment, such as paying of licenses and permits fees. Transformation maturity stage: is the advanced and more enhanced stage than stage three. Government operational processes are integrated and unified. Government systems are integrated at different levels between central, regional and local governments – vertically and horizontally. Available services include centralized government’s human resources and payroll systems. Continuous improvement maturity stage: is assumed to be the highest stage of e-government systems implementation and service delivery. More sophisticated technologies are used to enhance government service delivery and interaction with citizens. Government involves citizens in decision making and democratic processes activities such as political participation and online voting.

To integrate security services into the proposed eGMM – information security maturity models (ISMMs) were proposed as a tentative solution [12]. In the process, eight ISMMs were identified and extensively analysed for comprehensive security services. Models with orientations to management, evaluation and awareness were synthesized to form a comprehensive ISM with five critical maturity levels; Undefined, defined, managed, controlled, and optimized [12]:

Undefined maturity level: this is the lowest maturity level of information security model meant for organizations with low information security targets (IST) in a low security risk environment. Security policies may be available. Adequate user awareness is necessary. Security risk reduction from technical and non-technical security threats occurs. Defined maturity level: is the second maturity level meant for organizations with normal IST in a normal security risk environment. 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 embedded into organization culture. Managed maturity level: this is the more advanced level than level two. It is meant for organizations with high IST in a normal or high security risk environment. Also, high risk reduction from technical and non-technical security threats occurs. In addition, security policies including awareness, visions, and strategies are regularly reviewed and updated. Controlled maturity level: is the fourth maturity level of information security model meant for organizations with higher IST in a normal or higher security risk environment. Highest security risk reduction from technical and non-technical security threats occurs. Information security is embedded into the culture of the organization. Additionally, Security policies, awareness, visions, and strategies are regularly reviewed and updated. Optimized maturity level: this is assumed to be the highest maturity level. It is meant for organizations with higher IST in higher security risk environment. Higher security risk reduction from technical and non-technical security threats occurs. 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.

Thereafter, the proposed ISMM critical maturity levels [12] were integrated into eGMM maturity stages [13] to form a framework for securing e-government services which integrates IT security services into eGMMs maturity stages [11]. The figure below shows a graphical presentation of the framework. A developed catalogue of SRCAs is given in Annex–2.
What follows is a brief description on how the proposed framework (shown in figure 1) can be implemented to the government organisations. The proposed framework has two implementation phases (FIP–1 & 2). Phase one is meant for implementing e-government services marked as FIP–1, whilst phase two is meant for implementing security services for the identified e-government services in FIP–1, marked as FIP–2 [11]:

**FIP–1:** this phase is meant for getting familiarised with the framework on what it can do, and how it can be implemented. This phase is divided into two implementation steps marked as **FIS–1 & 2:**

**FIS–1:** Getting started – what the framework can do; this is the initial step, where organisations are getting familiarised with the framework. Using the framework organizations can achieve at-least the following:

- Understand what type of e-government services to be secured, why such services should be secured, how to secure such services, and to what degree/ maturity level;
- Establish the current status of e-government services and security services. The former is achieved through the use of the proposed maturity stages of eGMM and the latter is achieved through the use of the proposed ISMM critical levels;
- Develop requirements of security services strategic objectives for addressing e-government services strategic objectives at all phases: planning, development, implementation and service delivery;
- Use the framework as a checklist for guiding procuring entities of e-government services to easily identify, establish and plan for security services requirements of a given e-government project; and
- Enable government organizations to properly plan, manage, and monitor security services implementation and enhancement in compliance with security standards for e-government services that either exist or will later be in place.

**FIS–2:** Identify maturity stage/s for e-government services implementation; refers to the maturity stages of a common frame of reference for e-government maturity models (eGMMs): web-presence, interactional, transactional, transformational, and continuous improvement. At this step, e-government implementers will be able to clearly define the strategic objectives for e-government services to be implemented. This would include identifying type of e-government service, where it falls within the proposed maturity stages, identifying its functional requirements, and thereafter its implementation processes. Furthermore, e-government implementers will be able to plan for implementation of the same.

**FIP–2:** this phase is meant for implementing security services for the identified e-government services in phase one. The phase is divided into three implementation steps marked as **FIS–3, 4 & 5:**

**FIS–3:** Identify types of security services to be implemented; refers to the types of demanded security services requirement control areas (SRCAs) given in a catalogue, technical and/or non-technical. Technical security aspects include software and hardware solutions; and non-technical security aspects include ethical and cultural norms, legal and contractual documents, administrative and managerial policies, operational and procedural guidelines, and awareness programmes. Based on the earlier selected type of e-government services in FIS–2 – e-government implementers will be able to appropriately identify security services requirement, either technical and/or non-technical from a catalogue of SCRAs given in Annex–2.

**FIS–4:** Identify security services requirements control areas; refers to the demanded types of the security services requirement control areas (SRCAs) for either technical and/or non-technical: security objectives, security processes, and security metrics. Based on the selected type of security services in FIS–3 (either technical and/or non-technical) – e-government implementers will be able to strategically identify, establish and define appropriate security objectives, security
processes, and security metrics requirements from the catalogue of SCRAs given in Annex–2.

**FIS–5: Identify and selecting the required security maturity levels with their respective security services requirements control areas;** refers to the critical maturity levels of information security maturity model (ISMMs): undefined, defined, managed, controlled, and optimised.

It is important to note that ideally each of the five critical security maturity levels of ISMM has security maturity sub-levels within it: undefined, defined, managed, controlled and optimised. They are marked in figure 1 by capital letters (A–E, F–J, K–O, P–T, and U–Y) in the progression between one maturity sub-level to the other, and between one critical maturity level to the other. Definitions of the ISMM maturity sub-levels follow identically the definitions of the ISMM’s five critical maturity levels.

Security services requirement for critical maturity levels, such as that of the undefined level will be lower than that of defined level. Similarly, security services requirement for the defined level will be lower than that of managed level, and so on. The same ordering mechanism applies for ISMM security maturity sub-levels. It should be noted that based on the nature of e-government services (they are prone to current and emerging security risks and threats) – the framework components (security services requirements within the critical maturity levels and maturity sub-levels) were designed as an open system with feed-back mechanisms comprising of inputs, processes and outputs.

Therefore, e-government implementers will be able to strategically identify appropriate ISMM critical maturity level/s followed by the selection of the desired ISMM maturity sub-levels security services requirements from a catalogue of SCRAs given in Annex–2. Nonetheless, as the security services areas within the critical maturity levels and maturity sub-levels are in continuous progression, once the security maturity sub-levels of ISMM for a given e-government services is implemented – implementers will be able to improve security maturity sub-levels for the earlier selected e-government services by moving to the upper maturity sub-level/s within the critical maturity level using the same procedures.

Note however that, depending on the sensitivity of the selected e-government services (to be implemented and protected) organisations may not necessarily follow sequentially the ordering of the security maturity sub-levels within each critical maturity level of ISMM; i.e. one maturity sub-level after the other. They may skip some of the maturity sub-levels, but they will have to ensure that the security services requirements for the selected critical maturity level of ISMM are appropriately met.

One of the possible ways for measuring if levels of security services maturity, if it has been met, could be by conducting evaluations based on either security threat profile, security risk profiles or business impacts (balancing impact of security threats with safeguards).

**Framework limitations:** the authors acknowledge that currently the proposed framework has some limitations mentioned in the section for further research work.

### 3. Framework Evaluation Process and Methodology

Evaluation is the most important step in artifact development. An artifact could be a model, an instantiation or in this case a framework [6, 7]. The evaluation process provides essential feed-back to the framework development and quality assurance processes. The development process is iteratively performed until the real-world situation is improved. Evaluation methods includes observational, descriptive, analytical, testing and experimental [6, 7, 27]. Evaluation process could be categorised to investigate internal and external validity. Internal validity seeks for sound-able scientific basis though quality control of the internal processes of the proposed artifact, while external validity seeks for sound-able scientific basis though quality assurance if the proposed artifact meets the intended purposes [4, 6, 14].

Evaluation methods could be either practical, theoretical or both. **Practical evaluation** methods are testing, experimental and analytical. They involve use of quantitative techniques such as simulation, static and dynamic analyses, controlled experiments, and functional and structural analyses. These methods are good for conducting repetitive tasks by applying automated tools which take building and re-building phases out of the loop; also they deal with abstracting details and focus on functionality. However, practical evaluation methods may give wrong results due to incorrect input values [4, 6, 7, 14, 27]. Similarly, **theoretical evaluation** methods include observations and descriptions. They involve use of qualitative techniques such as case-study, field-study, informed argumentation and scenario analyses. These methods are good for evaluating text based information such as definitions and methodologies, detecting problem areas using different reviewers, and solving interpretation conflicts. But the methods appear to have poor control of the results for later replication [4, 6, 7, 14, 27].

Based on the above analysis, practical evaluation approaches require implementing the framework to the real-world environment; possibly by implementing a framework along with a given e-government project. The process will demand much time, and also larger resources. Therefore, as time limitation was the major factor in evaluating the proposed framework, at the moment, – theoretical evaluation approaches appears to be more appealing. As a result, a case-study was used for conducting a study. Case-study is an empirical inquiry that investigates a phenomenon within its real context; it relies much on multiple sources of evidence [18, 25]. We applied semi-structured interviews that involved use of pre-formulated questionnaire with provision for opinion/comments including allowing new questions to emerge during the interviews [18]. The targeted environment was the six government organisations studied earlier [10, 12].

The studied government organisations were [10, 12]: **Organisation U:** a ministry responsible for managing the overall revenue, expenditure and financing of the government; **Organisation V:** a ministry mandated to effectively administer land and human settlement development services; and **Organisation W:** 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 country-wide. The unit has now (2012) been effectively promoted to Agency level. 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: an agency charged with managing all ports and cargo in the country; and Organisation Z: an agency responsible for managing the assessment, collection and accounting of all central government revenues. The contacted groups were from different organisational levels: strategic (IT directors & decision/ policy-makers), tactical (IT managers & senior technical staff), and operational (IT technical staff responsible for implementing and/or managing e-government services). Respondents with less than 10 years of working experience in the area were regarded as Professionals, whilst those with more than 10 years of working experience in the area were regarded as Experts. The case-study was conducted in May, 2012.

4. Research Study: Data Collection, Processing and Analysis

Data collection, processing and analysis were divided into two major parts: the first part presents data collection processes, whilst the second part presents the research results from the processing and analyses of collected data.

4.1 Data Collection Process

To maintain consistency and continuity of our previous research study settings [10, 12] – we needed to use the same government organisations studied earlier.

Questionnaire preparation and testing process: questionnaire was prepared aimed at evaluating the proposed Framework. To be able to comprehensively evaluate the framework it was important to identify and develop evaluation criteria dimensions. Based on literature [4, 6, 7, 22, 27] seven framework evaluation criteria were developed. The criteria were: simplicity, coverage and completeness, compliance to security standards, and dynamics and flexibility. Others were: capability and relevance, usefulness, and trustworthiness; for details see Annex–1. For testing consistency and validity of the questionnaire a pilot study was conducted in the studied organizations via emails. The study focused to few selected personnel, one from each organization. Additionally, the study involved two experts from academia. After receiving responses from all respondents necessary improvements to the questionnaire were made. For filling in the questionnaire likert scale was used for rating the framework dimensions. The scale ratings were [14]: strongly disagree, disagree, not sure, agree, and strongly agree. Further, there were provisions within the questionnaires for respondents to give their opinions. Sample of the applied questionnaires are given in Annex–1.

Questionnaire distribution and data collection process: a total of 90 sets of the improved version of the questionnaire were physically re-distributed to the identified organizations. At each organization 15 respondents (2 at strategic level, 6 at tactical level, and 7 at operational level) were earmarked and given the questionnaire. In the process of conducting the interview respondents were briefed on the goal of the study, and also on how the proposed framework works. This information was also provided in the Annexes of the questionnaire. The undertaking took two weeks. A total of 69 (response rates 76.7%) of the filled questionnaires were collected from the surveyed organisations. The table below shows the matrix for the contacted and responded personnel within the studied organisations.

Table 1: Summary of respondents in the researched organizations

<table>
<thead>
<tr>
<th>Organization Name</th>
<th>Contacted Personnel (Professionals &amp; Experts)</th>
<th>Responded Personnel (Professionals &amp; Experts)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strategic Level</td>
<td>Tactical Level</td>
</tr>
<tr>
<td>U</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>V</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>W</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>X</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Y</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Z</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Total</td>
<td>12</td>
<td>36</td>
</tr>
</tbody>
</table>

4.2 The Results – Data Processing and Analysis

The collected data were cautiously processed and analyzed. Data processing and analysis process was categorized into descriptive and analytical data. Processing and analyzing descriptive data content analysis technique was used; whereas processing and analyzing analytical/simple statistical data Microsoft excel tool was used. Further, data processing and analysis undertaking were divided into three major parts: the first part analyses the frequency of acceptability, organizational-wise, for the proposed framework; the second part gives a comparative analysis on the degree of the framework acceptability among responders’ groups; strategic, tactical and operational levels; and the third part addresses framework’s areas of improvements which is based on the respondents’ opinions. However, due to paper space limitations – ratings for those who were either not sure, disagree or strongly disagree are not shown here.

4.2.1 Acceptability Ratings for the Proposed Framework

Research results for the acceptability ratings of the proposed framework are grouped into two categories: category–1 is the overall research results on the framework acceptability among the surveyed organisations; and category–2 is the detail research results on the framework acceptability among the surveyed organisations. The categories are presented as follows:

Category–1: Overall research results on the framework acceptability ratings: based on the established evaluation criteria – the analyses of the research results from the six surveyed organisations are discussed hereunder. Further, figure 2(a) below presents the summary of the research results:

Simplicity criterion: the overall acceptability rating was at 78% as depicted in figure 2(a). This suggests that respondents perceived the framework design to be clear and easily understandable to e-government implementers.
Coverage and completeness criterion: there was an increase on the overall acceptability rating of the framework under the criterion compared to the former one. The rating was at 88% as depicted in figure 2(a). This suggests that respondents perceived the framework to adequately address technical, non-technical, practice, and theory related security issues.

Figure 2(a): Overall acceptability ratings of the framework based on Agreed and Strongly agreed ratings

Compliance to security standards criterion: the overall acceptability rating was at 92% as shown in figure 2(a). This suggests that respondents perceived the framework to be aligned to the current security standards and best practices.

Dynamics and flexibility criterion: there was a decrease on the acceptability rating to around 76% compared to the former criterion as depicted in figure 2(a). This suggests that respondents fairly perceived the framework to be dynamic & flexible enough to deal with possible future security risks and threats facing e-government implementation and service delivery.

Capabilities and relevance criterion: there was an increase for acceptability rating under this criterion to around 77% compared to the former one as depicted in figure 2(a). This suggests that respondents perceived the framework to be feasible when dealing with security risks and threats facing e-government services.

Usefulness criterion: there was an increase for the acceptability rating to 95% compared to the former criterion as depicted in figure 2(a). This suggests that respondents perceived the framework to be useful when dealing with mitigating security risks and threats posed to e-government services.

Trustworthiness criterion: there was a decrease for the acceptability rating compared to the previous criterion of about 15%. The rating was at 80% as depicted in figure 2(a). Generally, respondents perceived that it is worth trusting the framework for mitigating security risks and threats facing e-government services.

Category–2: Detailed research results on the framework acceptability ratings: based on the established evaluation criteria – detailed analyses of the research results from the surveyed organisations are discussed hereunder. Further, figure 2(a) below presents the summary of the research results:

Simplicity criterion: detailed acceptability ratings compared among the six organisations showed that organization W appeared to have rated it at 99% followed by organization U at 92%. Organization Y appeared to have rated it lowest at 55%. This suggests that the framework design perceived to be clearer and easily understandable to personnel at organisation W than those at organisation Y. These differences amongst organisations could rely on many reasons including types of e-government services offered, and also personnel’s technical skills and expertise on security related issues.

Coverage and completeness criterion: detailed acceptability ratings compared among the six organisations showed that Organization X appeared to have highly rated it at 99%, followed by organization Y at 91%. Organization Z rated it the lowest at 80%. The results suggest that organisation X perceived the framework slightly more adequately addressing technical, non-technical, practice, and theory related security issues than organisation Z. Figure 2(b) below shows the detailed graphical view of the ratings.

Compliance to security standards criterion: detailed acceptability ratings compared among the six organisations showed that organizations V, W and X appeared to have rated it at around 100%; whilst organization U rated it the lowest at 75%. Higher ratings suggest that respondents perceived the framework to be more aligned with current security standards and best practices.

Dynamics and flexibility criterion: detailed acceptability ratings compared among the six organisations showed that organizations U appeared to have rated the highest at 99%; whilst organisation X rated it the lowest at 63%. This suggests that respondents at organisation U perceived the framework to be dynamic & flexible enough to deal with possible future security risks and threats facing e-government implementation and service delivery than those at organisation X.

Capabilities and relevance criterion: detailed acceptability ratings compared among the six organisations showed that organizations U appeared to have rated it highly at 92%; whilst organisation Y rated it the lowest at 64%. This suggests that
respondents at organisation U regard the framework to be more feasible when dealing with security risks and threats facing e-government services than those at organisation Y.

Usefulness criterion: detailed acceptability ratings compared among the six organisations showed that organisations U, W and X appeared to have rated it high at around 100%; whilst organization V rated it low at 85%. These results suggest that respondents at organisations U, W and X perceived the framework to be useful when dealing with mitigating security risks and threats posed to e-government services than those at organisation V.

Trustworthiness criterion: detailed acceptability ratings compared among the six organisations showed that organization W appeared to have rated it highly at around 90%; whilst organization V rated it the lowest at 62%. The results suggest that respondents at organisation W perceived that it is worthy trusting the framework for mitigating security risks and threats facing e-government services than those at organisation V.

4.2.2 A Comparative Analysis of the Framework Acceptability Ratings Among the Respondent Groups

A comparative analysis of the framework acceptability ratings among the respondents’ groups (strategic, tactical and operational levels) within the studied organizations are discussed below. Further, figure 3 presents the summary of the research results:

Simplicity criterion: there was fairly low variation of about 1% between the strategic and tactical levels. Further, there was slightly high variation of 14% between those at tactical and operational levels. This suggests that respondents at the strategic and tactical levels had more-less the same perception on the framework simplicity compared to those between strategic and operational levels. Figure 3 below shows the radar diagram of the results.

**Figure 3**: Comparative analysis for the framework acceptability among organizational levels: strategic, tactical and operational

Coverage & completeness criterion: there was fairly low variation of about 9% among the group levels between strategic and tactical. Also, variation between tactical and operational levels was at 11%. The implication here is that directors were more confidence with the framework security services coverage and completeness than managers and operational personnel. Figure 3 depicts the variation in detail.

Compliance to security standards criterion: there were fairly low variations among the group levels on the framework acceptability ratings. The variation between strategic and tactical levels was at 9%. Additionally, there was fairly very low variation of about 0.6% between tactical and operational levels. This suggests that respondents at the tactical and operational levels had similar perception on the framework compliance to security standards and best practices.

Dynamics and flexibility criterion: there were higher variations among the group levels on the framework acceptability ratings. Variation between strategic and tactical levels was at 38%; and that between operational and tactical levels was at 24%. This implies that personnel at the strategic level were more confidence than others; and that those at operational level were more confidence than those at tactical level. These perception gaps are well depicted in figure 3.

Capabilities and relevance criterion: there was higher variation in acceptability ratings for the framework among the group levels. Variation among strategic and tactical levels was at 19%; whilst that between tactical and operational levels was at 15%. This suggests that personnel at the strategic level were more confidence compared to those at the tactical and operational levels. Figure 3 shows the variation.

Usefulness criterion: there were fairly low variations among the group levels on the framework acceptability ratings. Between strategic and tactical levels the variation was at 6%. And between tactical and operational levels it was at 0.4%. This suggests that personnel at the strategic and operational levels had more-less the same perception level on the framework usefulness when dealing with security risks and threats facing e-government services.

Trustworthiness criterion: there was high variation in acceptability ratings for the framework among the group levels. The variation between strategic and tactical levels was at 19%; and that between tactical and operational levels was at 11%. This suggests that directors trusted more the framework than managers and supportive staff. Figure 3 depicts the variation in a radar diagram.

4.2.3 Analysis of the Frameworks’ Areas of Improvements

There were a number of feedback/ comments given by the respondents in the surveyed organisations. These comments were meant for improving the proposed framework. Therefore, the raised comments were analysed and summarized in Table 2. In the table, the first column gives the framework evaluation criteria. Second column narrates respondents’ raised comments in respect to framework areas of improvements. The last column summarizes measures taken to address the raised comments.

In the process, most of the raised comments were implemented to improve the proposed framework as indicated in the table under the column marked improvements made to...
the framework. Additionally, there were a few other comments that were not addressed in this paper, but will be considered for further research work. The table below narrates the analyses.

Table 2: Summary of Framework Evaluation Results

<table>
<thead>
<tr>
<th>Framework evaluation criteria and statements</th>
<th>Proposed areas of framework improvements</th>
<th>Improvement made to the framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplicity</td>
<td>Presentation of the selection matrix for security services needs to be simplified (figure 4–3), i.e. from FIS–4 to FIS–5]</td>
<td>Selection matrix for security services has been improved as depicted in figure 4. Each of the security service type (FIS–3) has its own security control area (FIS–4) and ISMM level (FIS–5).</td>
</tr>
<tr>
<td>Coverage &amp; completeness</td>
<td>To include SRCAs for the other ISMM sub-levels: defined, managed, controlled and optimized</td>
<td>SCRAs for the other ISMM sub-levels are considered for further research work</td>
</tr>
<tr>
<td>Compliance to security standards and best practices</td>
<td>To develop/ simplify the SRCAs structure/ architecture given in the Annex to the level that would easily be translated into actions by the personnel at the operational levels</td>
<td>Some of the SRCAs structures in Annex–2 have been simplified to the lowest level, such as CC and SSE-CMM. However, simplification of other SRCAs are considered for further research work</td>
</tr>
<tr>
<td>Dynamics &amp; flexibility</td>
<td>Establish possible way that would entail for appropriately easy selection processes for security services from the SRCAs catalogue when dealing with security risks and threats</td>
<td>Implementing measures that would provide greater objectivity in the selection and implementation processes of the SRCAs when securing e-government services. e.g. use of multi-criteria decision (MCD) methods is one alternative; this is considered for further research work</td>
</tr>
</tbody>
</table>

No comments were received in relation to the trustworthiness, usefulness, and capability & relevance criteria. The enhanced framework is shown in figure 4, along with a catalogue of security services requirements control areas (SRCAs) given in Annex–2.

5. Discussion

Generally, a total of 69 respondents in the surveyed organizations (the industrial representation) participated in the evaluation of the proposed framework (response rate=76.7). Based on the established evaluation criteria - respondents were very active in providing feedback/ comments on the areas of framework improvements. Collected data were categorized into analytical and descriptive data as presented in section 4.

Research results show that framework acceptability ratings were: 78% for simplicity, 88% for coverage and completeness, 92% for compliance to security standards, and 76% for dynamics and flexibility. Other ratings were: 77% for capability and relevance, 95% for usefulness, and 80% for trustworthiness. The acceptability ratings for framework’s usefulness and dynamics & flexibility being rated the highest and lowest respectively. Figure 2(a) & figure 2(b) depicts the overall and detailed acceptability ratings in graphical presentations respectively. Further, the analysis within the organizational levels (figure 3) showed that, personnel at the strategic level appeared to have a higher perception rate in accepting the framework than those at the tactical and operational levels.

Additionally, there were a number of feedback/ comments given by the respondents aimed at improving the proposed framework. Based on the analyses presented in section 4, the framework improvements were categorized into graphical presentation, and descriptive presentation. Graphically, the framework visualization was improved from the earlier version given in figure 1 to the current one given in figure 4 below.

The improvements made include simplification and enhancement of the selection process of security services requirement control areas (SRCAs) – where the linkages between FIS–4 and FIS–5 were improved by reducing the selection matrix arrows. Also, the word security was added at each of the three security services control areas given in FIS–4. In addition, the ISMM sub-levels (A–E, F–J, K–O, P–T, and...
U–Y) given in FIS–5 were re-organized within the ISMM critical levels to reflect the SRCAs selection matrix. Figure 4 shows the improved version of the framework

Descriptively, based on the given comments the catalogue of security services requirements control areas (SRCAs) was enhanced as shown in Annex–2. Some of the improvements made to SRCAs catalogue include enhancement of security elements from the Common criteria (CC) and the Systems security engineering capability maturity model (SSE–CMM). Nevertheless, other comments on the framework’s areas of improvement were not implemented at this phase due to several factors including time limitations. But they are taken for further research work. No feedbacks were given for improving the framework under the capability & relevance, usefulness, and trustworthiness criteria. The enhanced catalogue of SRCAs is given in Annex–2.

6. Conclusion and Further Research Work

The analysis of the collected data indicates that the framework is widely accepted by the respondents in the surveyed organizations. Respondents in the organisations at different levels (strategic, tactical, and operational) have high expectations that the framework would assist them in mitigating the current and emerging security risks and threats posed to e-government services. However, we acknowledge the limitation that the frameworks’ evaluation process employed only theoretical approach. Practical evaluation is also necessary before the framework can be generalized.

Therefore, further research work would focus into addressing the remaining issues given by the respondents on improving the framework. These issues include:

- Enhancing a catalogue of SRCAs for the intermediate security maturity sub-levels: undefined, defined, managed, and controlled;
- During the framework evaluation process it was observed that IT personnel at operational levels within the organizations, especially those with less years of working experience in the area of information security had difficulties to easily translate the framework SRCAs into implementation/ actions. Therefore, further research work could expand a catalogue of SRCAs to be more relevant to operational level;
- During the framework evaluation process it was observed that there was a perception gap on the security services adoption and use among the group levels within the surveyed organisations: strategic, tactical and operational levels. Therefore, investigating on how to bridge the current observed perception gap among the personnel at different organisation levels is another area that could be researched;
- The framework was qualitatively (theoretically) evaluated – further evaluation of the framework using quantitative (practical) methods is advised, in the same environment. Furthermore, the evaluation process of the framework (theoretically and practically) could be repeated in different environments, before generalization;
- Enhancing capabilities for calculating security services micro economic/ financial issues. The capabilities would enable organisations to cost–effectively establish appropriately the required security services budgeting issues for securing e-government services; and
- Establish a formal representation of the proposed framework. This would provide greater objectivity in the selection and implementation processes of the SRCAs when securing e-government services.

References

Appendices

**Annex–1:** Sample of the used questionnaire for evaluating the proposed framework

The description of the proposed framework for securing e-government services along with a catalogue of SRCAs is given in the Annexes of the questionnaire. Using the evaluation criteria given in the questionnaire kindly evaluate the proposed framework:

<table>
<thead>
<tr>
<th>Framework evaluation criteria &amp; description of the statements</th>
<th>Ranking Scale</th>
<th>Evaluators' self-assessment confidence level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplicity: The framework is designed in such a way that it is clear and easily understandable to e-government implementers.</td>
<td>Strongly Disagree</td>
<td>Strongly Agree</td>
</tr>
<tr>
<td>Comments:</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

| Coverage & Completeness: The framework adequately addresses technical security issues. | | |
| Comments: | | |

| | | | |
| | | | |

| | | | |
| | | | |

The graph below represents four areas that an ideal framework needs to cover: Technical complexity, social/non-technical complexity, practice complexity, and theory complexity. The components are given in ordinal scale 0 – 5, where 5 is the highest. As an example, the ideal framework would cover all the four areas at level 5 as shown in a quadrant form (with dotted lines) in the figure below. Please indicate, within the figure below, how well you see the proposed framework matches with the ideal one.

**Annex–2:** A catalogue of security services requirements control areas (SRCAs) for the proposed framework.

However, due to paper space limitations the improved version of the catalogue of security services requirements control areas (SRCAs) are not included here, but it is accessible through the following link: [http://people.dsv.su.se/karokola](http://people.dsv.su.se/karokola)