A Framework for Securing e-Government Services

The Case of Tanzania

Geoffrey Rwezaura Karokola

Doctoral Thesis in Computer and Systems Sciences at Stockholm University, Sweden 2012
A Framework for Securing e-Government Services

The Case of Tanzania

Geoffrey Rwezaura Karokola
Abstract

e-Government services are becoming one of the most important and efficient means by which governments (G) interact with businesses (B) and citizens (C). This has brought not only tremendous opportunities but also serious security challenges. Critical information assets are exposed to current and emerging security risks and threats. In the course of this study, it was learnt that e-government services, implementation and service delivery, are heavily guided and benchmarked by e-Government maturity models (eGMMs). However, the models lack built-in security services, technical as well as non-technical. They also measure quantity rather than quality of e-government services which leads to lack of strategic objectives alignment between e-government services and security services. Information security has an important role in mitigating security risks and threats posed to e-government services. Security improves quality of the services offered, and cuts across entire organisations. It requires involvement of employees at all levels: strategic, tactical and operational. Therefore, it is imperative that confidentiality, integrity and availability of critical information being stored, processed, and transmitted between G, B and C, become an integral part of e-government services, from planning, development, implementation, delivery, to maintenance phases.

In light of the above, the goal of this research work is to propose a framework that would facilitate government organisations to effectively offer appropriate secure e-government services. To achieve this goal, an empirical investigation was conducted in one of the developing regions in the sub-Saharan Africa; involving six Tanzanian government organizations. The investigations were inter-foiled by a sequence of structural compositions resulting in a proposition of a framework for securing e-government services which integrates IT security services into eGMMs. The framework will facilitate government organisations to effectively offer appropriate secure e-government services; hence contributing into formation of citizens’ trust, and consequently the success of e-government initiatives. The research work was mainly guided by a design science research approach complemented in parts by systemic-holistic and socio-technical approaches. Additionally, the proposed framework was qualitatively evaluated using criteria, such as simplicity, coverage and completeness, compliance to security standards, usefulness, and trustworthiness. The evaluation results indicated that the framework is highly accepted in the studied organisations at all levels. All major research results from the studies were reported in the research papers published at the appropriate peer-reviewed internationally recognised conferences and journals in information security and e-government.

The thesis contributes to the empirical and theoretical body of knowledge within the computer and systems sciences on securing e-government structures. It encompasses a new approach to secure e-government services incorporating security services into eGMMs. Also, it enhances the awareness, need and importance of security services to be an integral part of eGMMs to different groups such as researched organizations, academia, practitioners, policy and decision makers, stakeholders, and the community.
Sammanfattning


Avhandlingen utökar den empiriska och teoretiska kunskapsbasen för hur ämnesområdet data- och systemvetenskap kan bidra till att generellt säkra e-förvaltningsstrukturer genom att integrera informationssäkerhetstjänster i arbetet redan från planeringen av e-förvaltningssystemen. Avhandlingen kan också bidra till att förstärka medvetenheten hos viktiga intressentgrupper – till exempel beslutsfattare, politiker och samhället i stort - av behovet, betydelsen och nödvändigheten av att integrera säkerhetstjänster i eGMMs redan från arbetets början.
Acknowledgements

A journey of a thousand miles begins with a single step. Pursing a Doctorate of Philosophy degree (PhD) was always my dream and also a long term challenge. This dream would not have been achieved without the support and the kindness of many people around me.

Firstly and foremost, I would like to sincerely thank my main supervisor Professor Louise Yngström and my co-supervisor Associate professor Stewart Kowalski of the department of computer and systems sciences, DSV, (Stockholm University/Royal Institute of Technology, in Sweden) for their guidance, support, critique and encouragement that helps me to reach this stage. Additionally, I would like to extend my sincerely gratitude to Professor Paul Johannesson and Associate professor Christer Magnusson, of DSV, for their opponent role in particular during the defence of my Licentiate of philosophy degree. Additionally, my sincere gratitude goes to Associate professor Mikael Goldstein in Sweden. Furthermore, my sincere gratitude goes to Professor Beda Mutagahywa of the University of Dar es Salaam (Tanzania) for his valuable advice, encouragement and handling the programme coordination role, particularly during the empirical work in Tanzania. Also, my gratitude goes to Dr. Respickius Casmir of the University of Dar es Salaam.

Secondly, I would like to extend my gratitude to my colleagues and friends at DSV and the University of Dar es Salaam for their valuable support. Thanks to Rodolfo Candia, Birgitta Olsson, Fátima Ferreira, Lars Glimbert, Eija Jacklin, Tuija Darvishi, Marihan Ameen and others for handling administrative matter during the research period. Also, my extended appreciation goes to individuals and organisations located in Tanzania for their generosity and support during the empirical work; thank you so much.

Thirdly, it would have not been possible to undertake this research work without the financial support from the Swedish International Development Agency (SIDA) – sincerely thank you so much for funding this research work. Also, I am grateful to the University of Dar es Salaam for granting me this opportunity.

Lastly, I wish to express my gratitude to my family, to whom I dedicate this work.

— Thank You God —
Dedication

— To my Family —
Table of Contents

Part I:

1. INTRODUCTION AND BACKGROUND ................................................................. 1
   1.1 RESEARCH MOTIVATION AND PROBLEM AREA ........................................... 5
   1.2 RESEARCH GOAL AND RESEARCH QUESTIONS ............................................. 8
   1.3 LIST OF INCLUDED PUBLICATIONS .............................................................. 12
   1.4 THESIS STRUCTURE ...................................................................................... 13

2. RESEARCH METHODOLOGY .............................................................................. 15
   2.1 RESEARCH PHILOSOPHIES .......................................................................... 15
   2.2 RESEARCH APPROACHES ............................................................................ 17
   2.3 RESEARCH METHODS AND STRATEGIES ..................................................... 19
   2.4 RESEARCH SAMPLE SELECTION .................................................................. 21
   2.5 RESEARCH DATA COLLECTION, PROCESSING AND ANALYSIS TECHNIQUES ....... 23
     2.5.1 Study–1: Awareness of the Real-world Problem – Data Collection and Analysis .. 26
     2.5.2 Study–2: Suggestions for a Tentative Design – Data Collection and Analysis ... 28
     2.5.3 Study–3: Developing the Framework – Data Collection and Analysis .......... 29
     2.5.4 Study–4: Evaluating the Framework – Data Collection and Analysis ............ 31
   2.6 ETHICAL ISSUES CONSIDERATIONS ............................................................. 33
   2.7 CHAPTER SUMMARY .................................................................................... 34

3. THEORETICAL FOUNDATION FOR MODELLING E-GOVERNMENT SERVICES ...... 37
   3.1 UNDERSTANDING E-GOVERNMENT MATURITY MODELS AND THE PROBLEM AREA ... 37
   3.2 UNDERSTANDING INFORMATION SECURITY TERMINOLOGIES AND THEIR RELATIONSHIPS ... 38
   3.3 UNDERSTANDING THE CONCEPT OF SYSTEMS–THINKING AND HOLISTIC APPROACHES .... 40
   3.4 UNDERSTANDING MITIGATING MEASURES FOR IT SECURITY PROBLEM AREA ......... 48
     3.4.1 ISO/IEC 27000 Family: Code of Practice for Information Security Management ...... 48
     3.4.2 ISO/IEC 21827: Systems Security Engineering Capability Maturity Model ........ 49
     3.4.3 ISO/IEC 15408: The Common Criteria (CC) ............................................. 51
     3.4.4 National Institute of Standard and Technology (NIST) on e-Government ............ 52
     3.4.5 Information Security Management Maturity Model (ISM3) ........................... 53
   3.5 CHAPTER SUMMARY .................................................................................... 54

4. RESULTS – A FRAMEWORK FOR SECURING E-GOVERNMENT SERVICES ......... 57
   4.1 HOW THE FRAMEWORK WAS DEVELOPED ................................................ 58
   4.2 HOW THE FRAMEWORK WAS EVALUATED ............................................... 68
   4.3 HOW THE FRAMEWORK CAN BE IMPLEMENTED ........................................ 76
   4.4 CHAPTER SUMMARY .................................................................................... 79

5. SUMMARY OF THE INCLUDED PUBLICATIONS ................................................. 81
   5.1 SUMMARY OF RESEARCH PAPER I ............................................................. 81
   5.2 SUMMARY OF RESEARCH PAPER II ........................................................... 82
   5.3 SUMMARY OF RESEARCH PAPER III ......................................................... 83
   5.4 SUMMARY OF RESEARCH PAPER IV ......................................................... 84
   5.5 SUMMARY OF RESEARCH PAPER V ........................................................... 85
   5.6 SUMMARY OF RESEARCH PAPER VI .......................................................... 86
   5.7 SUMMARY OF RESEARCH PAPER VII ....................................................... 87
   5.8 CHAPTER SUMMARY .................................................................................... 88

6. CONCLUDING REMARKS AND FUTURE RESEARCH DIRECTIONS ................. 89
6.1 CONCLUDING REMARKS ........................................................................................................ 89
6.2 RESEARCH CONTRIBUTIONS ................................................................................................. 90
6.3 RESEARCH QUALITY AND TRUSTWORTHINESS ...................................................................... 92
6.4 RESEARCH LIMITATIONS AND FUTURE RESEARCH DIRECTIONS ........................................ 93

REFERENCES ........................................................................................................................................ 97

Part II: Publications

RESEARCH PAPER I .......................................................................................................................... 111
RESEARCH PAPER II .......................................................................................................................... 125
RESEARCH PAPER III .......................................................................................................................... 143
RESEARCH PAPER IV .......................................................................................................................... 169
RESEARCH PAPER V ........................................................................................................................... 183
RESEARCH PAPER VI .......................................................................................................................... 197
RESEARCH PAPER VII ......................................................................................................................... 209

Part III: Appendices

ANNEX A: LIST OF TERMS AND DEFINITIONS .............................................................................. 227
ANNEX A – 1: SYSTEMIC VIEW OF ICT, IT AND IS ................................................................. 227
ANNEX A – 2: DESCRIPTIONS OF CYBER-SECURITY ATTACKING TERMINOLOGIES .............. 228
ANNEX A – 3: OTHER E-GOVERNMENT DEFINITIONS .............................................................. 230

ANNEX B: ICT LANDSCAPING IN TANZANIA ............................................................................... 231

ANNEX C: A CATALOGUE OF SECURITY SERVICES REQUIREMENTS ........................................ 235

ANNEX D: LIST OF QUESTIONNAIRES – STUDY ONE ................................................................. 243
ANNEX D – 1: SAMPLE OF INTRODUCTION LETTER ................................................................. 243
ANNEX D – 2: RESEARCH QUESTIONNAIRE – STATE OF E-GOVERNMENT SECURITY ........ 244
ANNEX D – 3: RESEARCH QUESTIONNAIRE – SECURE E-GOVERNMENT ADOPTION ............ 254
ANNEX D – 4: EMMMS’ SECURITY SERVICES – EVALUATION CRITERIA ............................... 258

ANNEX E: LIST OF QUESTIONNAIRES – STUDY TWO & THREE ............................................... 264
ANNEX E – 1: SAMPLE OF INTRODUCTION LETTER ................................................................. 264
ANNEX E – 2: RESEARCH QUESTIONNAIRE – IDENTIFICATION OF ISMM SECURITY SERVICES .... 265
ANNEX E – 3: RESEARCH QUESTIONNAIRE – DEVELOPING A CATALOGUE OF SECURITY SERVICES REQUIREMENTS ................................................................. 267

ANNEX F: LIST OF QUESTIONNAIRES – STUDY FOUR ............................................................. 275
ANNEX F – 1: SAMPLE OF INTRODUCTION LETTER ................................................................. 275
ANNEX F – 2: RESEARCH QUESTIONNAIRE – EVALUATING THE PROPOSED FRAMEWORK ..... 276
List of Figures

Figure 1–1: Trends of ERI gap between developed and developing regions ........................................ 2
Figure 1–2: ERI statistics for regional, African regions, and Eastern African countries [UN, 2008] .................. 3
Figure 1–3: The security service gap for e-government services ................................................................. 4
Figure 1–4: Trends of attacking techniques – sophistication vs. attacker knowledge, adopted from Ciampa [2010, p. 6] .................................................................................................................. 6
Figure 1–5: Reported cyber-crime against financial losses [FBI, 2010] ...................................................... 7
Figure 1–6: Overview of the research motivation and problem area .............................................................. 8
Figure 1–7: Outline of the chapters in the thesis ......................................................................................... 14
Figure 2–1: Generic research onion process [Saunders et al., 2003] ......................................................... 15
Figure 2–2: Design research methodology, compiled from Vaishnavi & Kuechler [2004] ....................... 18
Figure 2–3: Overview of the research flow and inter-relationships ....................................................... 25
Figure 2–4: Extended generic research onion process with shaded research areas ............................. 34
Figure 3–1: Theoretical foundation sections inter-relationships ............................................................ 37
Figure 3–2: Security concepts and their inter-relationships [CC, 2009, p. 39] ........................................... 39
Figure 3–3: An open system within its environment [Schoderbek et al., 1985, p. 25] ............................. 41
Figure 3–4: A control system, simplified [Schoderbek et al., 1985, p. 104] ............................................. 42
Figure 3–5: Mapping of real-world environment into an open system .................................................. 43
Figure 3–6: Overview of systemic-holistic model [Yngström, 1996, p. 19] ............................................... 45
Figure 3–7: Detailed view of the systemic-holistic model [Yngström, 1996, p. 20] ................................. 45
Figure 3–8: Socio-technical model [Kowalski 1994, p. 10] ................................................................. 46
Figure 3–9: The SBC model [Kowalski, 1994, p. 19] ....................................................................... 46
Figure 3–10: SSE-CMM capability maturity levels [SSE-CMM, 2003, p. 44] .......................................... 50
Figure 3–11: CC development process [SANS, 2003b, p. 1] .................................................................. 51
Figure 4–1: A framework for securing e-government services which integrates IT security services into eGMMs (Version 2) ................................................................. 57
Figure 4–2: Integrating ISMM critical levels into eGMM stages ............................................................. 62
Figure 4–3: A framework for securing e-government services which integrates IT security services into eGMMs (Version 1) ................................................................. 66
Figure 4–4: Overall acceptability ratings of the framework using seven different evaluation criteria for all organizations (U – Z) ........................................................................ 66
Figure 4–5: Comparison of acceptability ratings of the framework using seven different evaluation criteria among organizations (U – Z) ......................................................... 70
Figure 4–6: Comparative analysis of framework acceptability ratings using evaluation criteria, among organizational levels: strategic, tactical and operational ....................................... 71
Figure 4–7: A framework for securing e-government services which integrates IT security services into eGMMs (Version 2) ................................................................. 76
Figure 6–1: Possible future overview of security services gap .............................................................. 90
Figure 6–2: Classification of the SEC 2000 proceedings [Björck & Yngström, 2001] with this research work contribution added as a big star ............................................................. 91
Figure 6–3: Technology adoption and security services gaps over time between G, B, and C ............. 95

List of Tables

Table 1–1: Summary of the research studies, questions and corresponding research papers .......... 11
Table 2–1: Matrix for the philosophical beliefs and perspectives ..................................................... 16
Table 2–2: Summary of IT personnel and overall work force in the selected organizations .......... 22
Table 2–3: Study–1. Number of respondents in the researched organizations .......................... 27
Table 2–4: Study–2. Number of respondents in the researched organizations .......................... 29
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2–5</td>
<td>Study 4, Number of respondents in the researched organizations</td>
<td>33</td>
</tr>
<tr>
<td>2–6</td>
<td>Extended table for research studies, questions, papers, and applied methods and strategies</td>
<td>35</td>
</tr>
<tr>
<td>3–1</td>
<td>Table 3-1: Sha guiding principles [Yngström, 1996, p.27]</td>
<td>44</td>
</tr>
<tr>
<td>3–2</td>
<td>Table 3-2: Matrix for research studies, applied methods, strategies, and holistic approaches</td>
<td>55</td>
</tr>
<tr>
<td>4–1</td>
<td>Table 4-1: Matrix for integrating SRCA into ISMM critical levels and EGMM stages</td>
<td>64</td>
</tr>
<tr>
<td>4–2</td>
<td>Table 4-2: Summary of a framework’s areas of improvements</td>
<td>74</td>
</tr>
</tbody>
</table>
## List of Acronyms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC</td>
<td>The Common Criteria</td>
</tr>
<tr>
<td>CCRA</td>
<td>Common Criteria Recognition Arrangement</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, Integrity and Availability</td>
</tr>
<tr>
<td>CMM</td>
<td>Capability Maturity Model</td>
</tr>
<tr>
<td>CMU</td>
<td>Carnegie Mellon University</td>
</tr>
<tr>
<td>CVS</td>
<td>Controlled e-Voting System</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DSR</td>
<td>Design Science Research</td>
</tr>
<tr>
<td>eGMM</td>
<td>e-Government Maturity Model</td>
</tr>
<tr>
<td>ERI</td>
<td>e-Government Readiness Index</td>
</tr>
<tr>
<td>e-Commerce</td>
<td>Electronic Commerce</td>
</tr>
<tr>
<td>e-Government</td>
<td>Electronic Government</td>
</tr>
<tr>
<td>e-Services</td>
<td>Electronic Services</td>
</tr>
<tr>
<td>FraSeGoS</td>
<td>A Framework for Securing e-Government Services</td>
</tr>
<tr>
<td>GP</td>
<td>Guiding Principles</td>
</tr>
<tr>
<td>GROP</td>
<td>Generic Research Onion Process</td>
</tr>
<tr>
<td>GST</td>
<td>General System Theory</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>ISMM</td>
<td>Information Security Maturity Model</td>
</tr>
<tr>
<td>ISM3</td>
<td>Information Security Management Maturity Model</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>ISO–27k</td>
<td>ISO 27002 family</td>
</tr>
<tr>
<td>ITSEC</td>
<td>Information Technology Security Evaluation Criteria</td>
</tr>
<tr>
<td>MDA’s</td>
<td>Ministries, Departments and Agencies</td>
</tr>
<tr>
<td>MITM</td>
<td>Man in the Middle</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnect</td>
</tr>
<tr>
<td>PBVS</td>
<td>Paper Based Voting System</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profile</td>
</tr>
<tr>
<td>QRM</td>
<td>Qualitative Research Method</td>
</tr>
<tr>
<td>QtRM</td>
<td>Quantitative Research Method</td>
</tr>
<tr>
<td>RQ</td>
<td>Research Question</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>SBC</td>
<td>Security By Consensus</td>
</tr>
<tr>
<td>SHA</td>
<td>Systemic–holistic Approach</td>
</tr>
<tr>
<td>SIDA</td>
<td>Swedish International Development Cooperation Agency</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SRCAs</td>
<td>Security services Requirements Control Areas</td>
</tr>
<tr>
<td>SSE-CMM</td>
<td>Systems Security Engineering Capability Maturity Model</td>
</tr>
<tr>
<td>SSM</td>
<td>Soft Systems Methodology</td>
</tr>
<tr>
<td>STA</td>
<td>Socio-technical Approach</td>
</tr>
<tr>
<td>TAM</td>
<td>Technology Adoption Models</td>
</tr>
<tr>
<td>TISS</td>
<td>Tanzania Inter-banking Settlement System</td>
</tr>
<tr>
<td>TNGS</td>
<td>Tanzanian National e-Government Strategy</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-site Scripting</td>
</tr>
<tr>
<td>24/7</td>
<td>Round the clock service</td>
</tr>
</tbody>
</table>
Part I
Chapter 1

1. Introduction and Background

The advances in information and communication technology (ICT)\(^1\) have made many electronic services possible. The services are often referred to with the prefix “e”, for example e-Commerce for electronic commerce services, e-Banking for electronic banking services, e-Learning for distance learning services, and e-Government for electronic government services. The concept of e-government has been given many definitions depending on the perspective and background of the interpreter. Brawn and Brudney [2001], Busu [2004], Mean and Schneider [2000], UN [2008], and the WorldBank [2002] all define e-government in different ways. In this thesis the WorldBank [2002, p.2] definition is chosen because it gives a wider and broader purpose about e-government. e-Government is the “government-owned or operated systems of information and communication technologies that transform relations with citizens (C), the private sector (B) and/or other government agencies (G) so as to promote citizens’ empowerment, improve government efficiency and service delivery, strengthen accountability and increase transparency”. Further, the definition\(^2\) implies that e-government promote services integration and availability 24/7, improves overall governance and active participation of citizens in public decision-making processes, and reduces unnecessary travel and service costs. Also, e-government is said to reduce corruption, and minimize the use of paper based procedures, thus improving socio-economic development [Baum et al, 2000; Brudney et al, 2001; UN, 2008; WorldBank, 2001, 2002].

In this regard, e-government services have become one of the most important and efficient means by which governments (G) can interact with citizens (C) and businesses (B). Additionally, based on the nature of e-government inter-relationships, they are categorized into internal and external. The former refers to Government to Government (G2G), Business to Business (B2B), and Citizen to Citizen (C2C). The latter refers to Government to Business (G2B), Government to Citizen (G2C), and Business to Citizen (B2C) [Mean et al, 2000; WorldBank, 2001, 2002].

To guide and benchmark e-government implementation and service delivery, 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, degree of technology complexity, degree of system sophistication, and the level of interaction with users [Gronlund et al, 2005; Moon, 2002; WorldBank, 2001, 2003]. It is broadly recognized that the advantage of having a

---

\(^1\) Definitions about ICT, IT and IS are discussed in Annex A–1.

\(^2\) Other e-government definitions are given in Annex A–3.
stage-wise approach is to offer the government the ability to measure the progress of e-government implementation and service delivery, giving it the flexibility to develop and prioritize e-government-related projects and activities, and facilitating organizations to meet e-government goals by ensuring that business and technological components are effectively aligned [Gronlund et al, 2005; Layne et al, 2001; UN, 2008; WorldBank, 2003]. A more detailed analyses and discussion about eGMMs is given in Part II of this thesis as research paper III [Karokola et al, 2012a].

The UN [2008] e-government survey report shows that whilst most of the developed regions appeared to be at mature stages of, implementation and service delivery of e-government services, the majority of the developing regions (countries) are at infancy stages [Heeks et al, 1999b; UN, 2008]. In addition, the report shows that the e-Government readiness index (ERI) gap between the two regions is widening, as shown in figure 1–1 below.

![Figure 1–1: Trends of ERI gap between developed and developing regions](image)

Further, the report shows that Europe was ranked highest with an e-readiness index of 0.6490, followed by Americas (0.4936), Asia (0.4470), Oceania (0.4338) and Africa (0.2739). Additionally, because this research is focusing on one of the developing countries (Tanzania) located in the Eastern African region, it was important to investigate the ERI gap further. Within African regions the statistics

---

3 Developing Countries are characterized by low income per capital i.e less than US$ 1 per day, low human development index (HDI), low human life expectancy, and low Gross domestic product (GDP) [WorldBank, 2008]. In this thesis the word developing countries, and developing regions are used interchangeably.

4 e-Government readiness index is a comparative ranking of the Countries in the world according to their level of e-government (digital) services. It involves two primary indicators: the state of e-government readiness, and the extent of e-participation. e-Government readiness is the ability to use ICT to develop one’s economy and to foster one’s welfare [UN, 2008].

5 Americas are countries located in Central, Southern, Northern American and Caribbean [UN, 2008].

6 Oceania are countries such as Australia, New Zealand, Fiji, Samoa, Marshall Islands [UN, 2008].
shows that Southern Africa was ranked highest with an e-readiness index of 0.3893, followed by Northern Africa (0.3403), Eastern Africa (0.2879), Central Africa (0.2530), and Western Africa (0.2110). Country-wise in the Eastern Africa, Kenya was ranked highest with an e-readiness index of 0.3474, followed by Uganda (0.3133), Rwanda (0.2941), Tanzania\(^7\) (0.2929), and Burundi (0.1788) [UN, 2008, pp.19–40]. ERI statistics are graphically presented for Regional, African regions and Eastern African countries in figure 1–2 below.

![Figure 1–2: ERI statistics for Regional, African regions, and Eastern African countries](UN, 2008)

To bridge the e-government services gap between the regions, developing countries are heavily investing into the adoption\(^8\) and use of more sophisticated e-government services. In doing so they face a number of challenges related to technological, as well as non-technological issues. Some of the technological related issues were existence of un-favourable environmental conditions, context between systems designers and the environment in which the systems are implemented, poor broadband internet access, limited access and late adoption to new technologies, and lack of knowledgeable and skilled IT personnel to support the services. Other issues were security related issues, technical and non-technical\(^9\). Contrary to developing countries, implementation of e-government services in the developed countries started gradually to give room for consideration of mitigating many of the challenging aspects, including IT security related issues. Also for developing countries, some of the non-technological related issues were lack of adequate resources for building a nation-wide ICT support infrastructure, inadequate training of personnel for supporting e-government initiatives, and lack of proper legal framework to protect electronic data. Other issues were mushrooming of un-coordinated and duplicated e-government initiatives, which resulted in loss of financial resources; and poor political stability and structure [Bakari, 7

---

\(^7\) Tanzania is one of the developing countries located in the Sub-Saharan Eastern Africa with a population of about 41million and tele-density of about 43% [TCRA, 2010]. The ICT landscaping in Tanzania are given in Annex B.

\(^8\) Adoption refers to acquisition and deployment of technologies

\(^9\) Non-technical and social-technical are used interchangeably, definitions are given in chapter 1.1, para 1.
In investigating further into security related issues as one of the challenges affecting secure e-government services, it appears that by implementing more sophisticated services, mission-critical information assets\(^{10}\) and infrastructure are exposed to more, and in some cases to new security risks\(^{11}\) and threats. Customarily, before this intervention, interaction between governments (G), businesses (B) and citizens (C) requires physical visits to government offices or use of physical mail services that pose traditional and well known threats to paper-based information assets. e-Services\(^{12}\) create new security challenges to e-government domains (G, B, C) [Hwang et al, 2004; Karokola et al, 2009a, 2012a; Wimmer et al, 2002].

Figure 1–3 below shows e-government service sophistication, implementation and service delivery, as a function over time. The security services gap (technical and non-technical) for securing e-government services is also shown as a function over time. The gap appears to be systemic in nature as pointed out, among others, by Kowalski [1994] and Bakari [2007] and is widening, unless appropriate measures are taken.

Figure 1–3: The Security service gap for e-government services

Information security is an essential tool for managing security risks and threats in any environment. Information security is a quality issue that cuts across the entire organization. It requires involvement of employees at all levels (strategic, tactical and operational)\(^{13}\). Information security is driven by a set of objectives and improves the

---

\(^{10}\) Assets refers to entities that someone places value upon [CC, 2009].

\(^{11}\) Security risks, threats and vulnerabilities are described in chapter 3.2.

\(^{12}\) e-Services refers to provision of electronic services that reflect three main actors: service provider, service receiver and the channels of service delivery. Also, the terms accommodates e-government and e-commerce services [Wiki, 2011].

\(^{13}\) Organization levels are defined in chapter 2.5, third bullet.
quality of the offered service [ISM3, 2007]. Security ensures confidentiality\(^{14}\), integrity\(^{15}\), and availability\(^{16}\) of critical information assets being stored, processed, and transmitted within and between e-government domains [Karokola et al, 2009a, 2012a; Martins et al, 2002; Woodhouse, 2008b; Yngström, 1996; Zhou et al, 2008]. 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 [UN, 2008; West, 2004; Wimmer & Bredow, 2002].

In response to the security services requirements gap in e-government services – several attempts have focused on developing approaches that would bridge the security service gap and mitigate current and emerging security risks and threats. However, recent studies [Bakari, 2007; Casmir, 2005; Chaula, 2005; Grant et al, 2005; Hwang et al, 2004; Karokola et al, 2008, 2009a; Martins et al, 2002; Tarimo, 2006; Wimmer et al, 2002; Woodhouse, 2008a; Zhou et al, 2008] have shown that securing systems such as e-government services is still a challenging and urgent issue that requires a variety of approaches [Busu, 2004; Lambrinoudakis et al, 2003; Wimmer et al, 2002].

The rest of the chapter is organized as follows: the chapter presents research motivation and problem area, followed by research goal and research questions, and summary of the included publications. Finally, the chapter concludes by presenting an outline of the thesis structure.

1.1 Research Motivation and Problem Area

Given the fact that bridging the existing e-government security service gap between developed and developing-countries, security-service related issues appear to be one of the challenges affecting the implementation and delivery of secure e-government services. As a result, critical information assets and/or the underlying infrastructure are exposed to more and in some cases to new security risks and threats. Security threats pose many security challenges to organisations and e-government services. They exploit specific vulnerabilities affecting confidentiality, integrity, availability, and accountability\(^{17}\) of e-government critical information assets [Grant et al, 2005; Lambrinoudakis et al, 2003; Zhou et al, 2008]. At the abstract level security threats posed to e-government services could result from technical and/or non-technical related issues. Technical security aspects may include vulnerability caused by poor system design, development, implementation, configuration, integration (vertical and horizontal)\(^{18}\), and/or maintenance. Similarly, non-technical security aspects may result

\(^{14}\) Confidentiality refers to concealment of information resources by preventing disclosure or exposure to unauthorized individual or systems [Bishop, 2006].

\(^{15}\) Integrity refers to the trustworthiness of data or resources (preventing improper or unauthorized change) [Bishop, 2006]

\(^{16}\) Availability is defined as state of information being accessible for use without interference or obstruction when needed

\(^{17}\) Accountability is defined as the ability to trace performed activities to someone responsible [Bishop, 2006].

\(^{18}\) Vertical integration refers to e-government services integration between lower and higher levels, i.e. G2C; whilst Horizontal integration refers to e-government services integration between same levels, i.e. G2G [WorldBank, 2001].
from lack of ethical and cultural norms, legal and contractual documents, administrative and managerial policies, operational and procedural guidelines, and/or awareness programmes [Gil-Garcia et al, 2005; Kowalski, 1994; Martins et al, 2002; Michael et al, 2009; Wimmer et al, 2002; Yngström, 1996].

A study conducted by the Carnegie Mellon University (CMU) from 1994 – 2003, revealed that cyber attacking tools have become more sophisticated and readily available. Consequently, low knowledge is required for an intruder to attack a system. Identified dangerous sources of security threats/cyber-crime attacks include: cross site scripting (XSS), remote command execution, SQL injection, man-in-the-middle (MITM), weak authentication, information disclosure, information manipulation, distributed denial of service (DDoS) and malicious code/virus (Trojan horses, worms and spy-wares). Further, the statistics showed that for the year 2003 the number of reported security incidents increased to 137,000 out of 215 million hosts (users). Figure 1–4 below depicts the trend of cyber-attack sophistication versus the required knowledge of attackers over time.

![Figure 1–4: Trends of attacking techniques – Sophistication vs. attacker knowledge, adopted from Ciampa [2010, p. 6]](image)

The Federal bureau of investigation (FBI) cyber-crime report shows that the number of reported complaints against the amount of financial losses is increasing yearly. The reported total financial losses for the year 2005 amounted to 183.12

---

19 Cyber-crime refers to on-line criminal activities that make use of computers, networks and the internet for committing crimes [FBI, 2010].

20 Definitions for the given terms used in Cyber-security attacking techniques are described in Annex A–2.
million US$, whilst for year 2009 financial losses rose to the amount of 559.7 million US$ [FBI, 2010]. Figure 1–5 below depicts the cyber-crime trends over time.

![Figure 1–5: Reported cyber-crime against financial losses [FBI, 2010]](image)

In Tanzania, the Citizen [2009] reported one of the largest cyber-crimes in the country. The attacker took advantage of the newly established Tanzanian inter-banking settlement system (TISS) for electronic money transfer to embezzle more than 5 million US$ remitted electronically by one of the state organizations to the Revenue authority. This is an example of how large and complex the security problem in e-government services is.

The Tanzanian national e-government strategy (TNGS) recognizes the importance and use of e-government maturity models (eGMMs) for guiding and benchmarking e-government implementations and service delivery. It suggests the use of eGMM with maturity stages similar to Gartner’s model [Karokola et al, 2009a, 2012a; Tz-eGov, 2008]. However, the findings from a comparative analysis of the internationally recognised eGMMs show that they lack security services, technical and non-technical, in their maturity stages [Karokola et al, 2012a]. As a result, often, security services have not been considered in the early stages, such as during the planning, development, implementation, service delivery, and maintenance phases of e-government projects. This implies that eGMMs were designed to rather measure the quantity than the quality of e-government services offered; leading to misalignment of strategic objectives between e-government services and security services. Thus, it is argued that security services should be considered at the early stages of IS/IT/ICT systems development such as e-government services. Additionally, as underlined before, e-government services create new security challenges to government, business and citizens. Therefore an increased variety\(^{21}\) of security services is required [Busu,

---

\(^{21}\) Variety is the minimum number of states that is necessary to control a system of a given number of states; Ashby law of requisite variety "only variety can destroy variety" [Schoderbek et al, 1985].
Additionally, the Tanzanian national e-government strategy does recognise security and privacy as one of the key guiding principles for success of e-government services. Other guiding principles are given in Annex B of this thesis [Tz-eGov, 2008, p. 9]. Yet, there exist a number of information security models, frameworks, and best practices (some are presented in chapter 3) still it is very challenging undertaking for the studied Tanzanian organizations to effectively and appropriately secure e-government services [Karokola et al, 2009a, 2010, 2011a, 2012a].

When responding to these challenges it is imperative that security services becomes an integral part of the eGMMs stages, so as to bridge the security service gap; consequently, securing e-government services before it is too late. Figure 1–6 below presents a schematic overview of the research motivation and problem area.

![Figure 1–6: Overview of the research motivation and problem area](image)

In the figure above, the box to the left shows the areas of focus, eGMMs and IS/IT security services for mitigating security risks and threats posed to e-government services. The box in the middle shows eGMM integrated with security services (a secured eGMM); and the box to the right shows the expected overall result (secured e-government services).

1.2 **Research Goal and Research Questions**

Government organizations have different objectives, are custodians of different assets, offers different e-government services, and face different security risks and threats at different levels. Therefore they do require different varieties of security services [ISM3, 2007; ISO-27K, 2005; Karokola et al, 2011a; NIST, 2007a; Schoderbek et al, 1985]. The research findings, discussed above and in research papers I, II and III, show that government organisations are facing a number of challenges when offering suitable variety of secure e-government services. One of the identified challenges was...
the lack of built-in security services in the maturity stages of eGMMs [Karokola et al, 2012a].

Bridging the current security service gap in eGMMs would result into providing measures for both quantity and quality of offered e-government services; by ensuring that the strategic objectives between e-government services and security services are effectively aligned during the planning, development, implementation, service delivery, and maintenance phases. Consequently, enhancing confidentiality, integrity and availability of critical information assets being stored, processed, and transmitted within and between e-government domains (G, B and C).

Therefore, the goal of this research work is to propose a framework that would facilitate government organisations to effectively offer appropriate secure e-government services.

To better understand the scope and magnitude of the research goal – four research studies along with their respective research questions were formulated as follows:

**Study–1: Research question (RQ) 1**

At first, it was important to identify and establish the magnitude of the real-world problem, including current practices used in securing e-government services. When responding to these requirements, research question RQ 1 was split into two sub-research questions:

The first sub-research question aimed for establishing the real-world problem in securing e-government services. It involved investigating the current e-government services status, security issues and challenges, and security measures used in the studied environment. Therefore, the first sub-research question RQ 1(a) was formulated as:

(a) *What are the current issues and challenges facing secure e-government services, implementation and service delivery, in the study environment?*

⇒ This sub-research question is answered in research papers I and II where government organizations were studied. The findings revealed that security services for securing e-government services are implemented in an ad-hoc manner. Additionally, it was learnt that e-government services, implementation and service delivery, are heavily influenced by eGMMs which appear to lack built-in security services. Further, it was learnt that some respondents regarded that if the said model/s could have built-in security services, perhaps, it could improve the situation. This triggered for further investigation regarding security services in eGMMs.

Based on the findings from RQ 1(a), in particular those that relate to lack of security services in eGMM, it was necessary to conduct a more elaborative analysis on
the currently used eGMM in the studied environment. Additionally, it was imperative to identify and investigate other internationally recognised eGMMs for security services. Therefore, the second sub-research question RQ 1(b) was formulated as:

\[(b) \text{What are the strengths and weaknesses, technical and non-technical, of the IT security services defined in internationally recognised eGMMs?}\]

\[\Rightarrow \text{This sub-research question is answered in research paper III whereby ten more internationally recognised eGMMs were identified and extensively analysed. The findings show that all eleven eGMMs lacks built-in security services, technical and non-technical, in their maturity stages. Additionally, it was learnt that eGMMs were structured differently, stage-wise. So structurally models were synthesized whereby five maturity stages for a common frame of reference for eGMMs were proposed.}\]

**Study–2: Research question (RQ) 2**

After study–1, it was imperative to investigate, identify, and develop security service measures, technical and non-technical, that could appropriately be integrated into the maturity stages of eGMMs, proposed in RQ 1(b) and outlined in research paper III. Therefore, the second research question RQ 2 was formulated as:

\[\text{What contemporary IT security services could appropriately be integrated into the proposed maturity stages of eGMMs for securing e-government services?}\]

\[\Rightarrow \text{This research question is answered in research paper IV, where various information security maturity models (ISMMs) were identified and selected as the possible appropriate measures for the identified security problem. ISMMs were selected because the orientation of their security services critical}\textsuperscript{23} \text{maturity levels are designed in a continuous incremental order from a low to high ones; which is similar to e-government services within the maturity stages of eGMMs. In the process, eight internationally recognized ISMMs were selected and analysed for security services enhancement. The models were then synthesized and five critical maturity levels of ISMM were proposed. The development process of the enhanced ISMM was followed by a survey study that aimed at affirming the proposed critical maturity levels and the corresponding security service requirements control areas, technical and non-technical.}\]

**Study–3: Research question (RQ) 3**

After study–2, which identified which IT security services that are appropriate, it was necessary to develop a framework for integrating the ISMM security services proposed in RQ 2, outlined in research paper IV, into the maturity stages of the eGMM, proposed

---

\textsuperscript{23} The word “critical” in ISMM imply that these maturity levels are necessary to be followed sequentially because they builds on each other [NIST, 2007b].
in RQ 1(b), outlined in research paper III. Therefore, the third research question RQ 3 was formulated as:

*How can the proposed ISMM security services be appropriately integrated into the proposed eGMM to form a framework for securing e-government services?*

 ⇒ This research question is answered in research paper V, whereby a framework for securing e-government services which integrates IT security services into the five stages of the eGMM was proposed. In the paper the framework development process is presented; where the proposed framework is presented in a pictorial orientation, along with a catalogue of security services requirement control areas (SRCAs) for both technical and non-technical.

**Study–4: Research question (RQ) 4**

After study–3, it was necessary to evaluate the proposed framework, addressed in RQ 3 and outlined in research paper V, in the studied environment. Therefore, the fourth research question RQ 4 was formulated as:

*How can the proposed framework be evaluated to effectively and appropriately meet the demands for secure e-government services in the studied environment?*

 ⇒ This research question is answered in research papers VI and VII. In the papers, research results from the framework evaluation and testing process are presented. The results show that the proposed framework was widely accepted by the respondents within the surveyed organisations at all levels: strategic, tactical, and operational.

Table 1–1 below summarizes the presentation of this section. In the table, the linkage between research study, research question, and the corresponding research paper is given. Also, the titles of the published research papers are listed in chapter 1.3.

**Table 1–1: Summary of the research studies, questions and corresponding research papers**

<table>
<thead>
<tr>
<th>Research study</th>
<th>Research Questions</th>
<th>Corresponding research papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1(a)</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>1(b)</td>
<td>II</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>IV</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>V</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>VI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VII</td>
</tr>
</tbody>
</table>
1.3 List of Included Publications

The following is the list of included research papers published in peer-reviewed internationally recognised conferences and journals in the area of information security and e-government. Extended summaries of the research papers are given in chapter 5. Also, full research papers are included in Part II of this thesis:

Paper I:

Paper II:

Paper III:

Paper IV:

Paper V:

Paper VI:
Paper VII:

The following publications were not included in this thesis:
Licentiate Thesis:

Paper VIII:

Paper IX:

1.4 Thesis Structure
This thesis comprises of six chapters. The chapters are organized in the following order:

Chapter 1: presents the introduction and background to the research area. This is followed by the research motivation and problem area; research goal, research studies and their corresponding research questions. Finally, a list of the included peer-reviewed publications is given.

Chapter 2: presents the research methodology and its mechanisms. It begins by giving an overview of philosophical assumptions. These are followed by research approaches, research methods and strategies. Additionally, the research sample selection; data collection, processing and analysis technique; and ethical issues are outlined. Finally, a chapter summary is presented.

Chapter 3: presents the theoretical foundation and related work for modelling information security and e-government services. The chapter provides a description of
the underpinnings of e-government maturity models and their problem area in relation to security services, and understanding of IT security terminologies in e-government services and security. In addition, the chapter provides the theoretical understanding of systems-thinking and holistic approaches, and security standards and best practices in information security maturity models. Finally, a chapter summary is presented.

Chapter 4: presents the research results. In this chapter, a summary description on how the framework was developed is outlined. Further, a summary description on how the framework was evaluated, and how it can be implemented into organizations is presented. Lastly, the chapter summary is given.

Chapter 5: presents an extended summary of the included research papers published in peer-reviewed internationally recognized conferences and journals in information security and e-government. Full research papers are provided in Part II of this thesis.

Chapter 6: presents the concluding remarks. In the chapter, research contributions, and research quality and trustworthiness are outlined. Further, research limitations and future research work is discussed.

Figure 1–7 below shows outline of different chapters and their inter-relationships.
Chapter 2

2. Research Methodology

Given the nature of this research work, it was imperative to identify and apply suitable research approaches that are well structured, comprehensive and elaborative. As a result, a generic research onion process (GROP), shown in figure 2–1 below, was adopted to guide this research work [Saunders et al, 2003].

![Figure 2–1: Generic research onion process [Saunders et al, 2003]](image)

The GROP has the following layers: research philosophies and research approaches, research methods (choices) and strategies, research time horizons, and data collection and analysis techniques.

What follows is the description of how these research layers were applied in this research work. Additionally, outlines of the research sample selections, ethical issues, and a chapter summary are given.

2.1 Research Philosophies

Research refers to activities or processes that scientifically contribute to the discovery and confirmation of knowledge. Knowledge is obtained through the use of appropriate philosophical assumptions about the techniques used in relation to the researcher’s
perspective. The researcher makes claims about what is the nature of knowledge (ontology), how it is known (epistemology), what values it holds (axiology), and what are the processes for studying it (methodology) [Dawson, 2002; Myers, 2009; Vaishnavi et al, 2004; Yin, 1994].

In this research work, the author attempts to pursue the positivist and interpretive philosophical assumptions, given in GROP layer one, figure 2–1. Positivism is the form of research that assumes reality is objectively given, and is described by measurable properties which are independent of the researcher. It involves testing of theories in an attempt to increase predictive understanding of the phenomena. Also, it includes formulating propositions that portrays the subject matter in relation to independent and dependent variables and the relationships between them. Similarly, Interpretivism assumes that access to reality is subjective, and is given through social constructs. Contrary to positivism, interpretivism does not predefine independent and dependent variables, but rather attempts to understand phenomena through the complexity of meanings that people may assigned to them [Myers, 2009; Robson, 2002; Saunders et al, 2003; Yin, 1994]. To better understand these philosophical terms, they are analysed in the table below. Table 2–1 is divided into philosophical beliefs and philosophical perspectives.

Table 2–1: Matrix for the philosophical beliefs and perspectives

<table>
<thead>
<tr>
<th>Philosophical Beliefs</th>
<th>Philosophical Perspective</th>
<th>Positivist</th>
<th>Interpretive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epistemology</td>
<td>Objective, detached observer of truth, dispassionate</td>
<td>Subjective, (values and knowledge emerge from the researcher-participant interaction)</td>
<td></td>
</tr>
<tr>
<td>Ontology</td>
<td>A single reality, probabilistic</td>
<td>Multiple realities, socially constructs</td>
<td></td>
</tr>
<tr>
<td>Axiology</td>
<td>Testing of hypothesis (Truth, Prediction)</td>
<td>Explorative (understanding situation and description)</td>
<td></td>
</tr>
<tr>
<td>Methodology</td>
<td>Observation, quantitative, statistical</td>
<td>Participation, qualitative, hermeneutical,</td>
<td></td>
</tr>
</tbody>
</table>

Adopted from [Dawson, 2002; Myers, 2009; Vaishnavi et al, 2004; Yin, 1994]

The goal of this research work is to develop a framework that would facilitate government organisations to effectively and appropriately secure e-government services. Therefore, to effectively achieve this research goal – it is important to explicitly understand the real-world problem (in-secure e-government services), using multiple realities from which knowledge may emerge. The real-world environment is represented by the selected organisations (discussed in chapter 2.4), which are represented by individuals within the organisations. Therefore, interpretivism was chosen as the relevant philosophical assumptions to guide this research work.
2.2 Research Approaches

Knowledge development could be achieved through the use of a suitable research approaches. Different research approaches were the main pillars used to guide this research work. They were used to identify, select, and develop suitable research design, strategies and techniques for data collection, processing and analyses. Looking at GROP layer two shown in figure 2–1 research approaches are of deductive and/or inductive type [Pierce, 1931; Saunders et al, 2003].

Deductive research processes are associated with generating knowledge from theory. Also, deductive research depends much on the experimental design approach that mostly involves collection of quantitative data. Deductive research processes are also suitable for generalization of the artifact [Pierce, 1931; Saunders et al, 2003]. Contrary to deductive research processes, inductive research processes emphases a deeper understanding of the real-world problem. Usually the researcher becomes part of the research process, and it involves the use of qualitative data. Also, it helps in developing design structures (artifacts), and the construction of cases/ scenarios [Pierce, 1931; Saunders et al, 2003]. Inductive research is associated with an abductive research process. Abductive refers to the process of extracting causal relationships from data generation and analysis to the development of artifacts or theories. The process is repetitively done [Pierce, 1931; Vaishnavi et al, 2004]. Based on the above analysis, an inductive research process appeared to be in line with the research goal of this research work. Consequently, it was chosen to guide this research work.

Further, it was imperative to establish suitable research approaches that are in line with an inductive research process. Based on the research goal, the following criteria for research approaches selection were formulated: the approach should be capable of merging different studies aimed at addressing one common research goal, such as developing a framework; it should be capable of modelling e-government services, e-government maturity models, and information security maturity models; and it should be capable of designing (developing and evaluating) a framework. As a result, design science research process was adopted.

Design science research (DSR) methodology can be conducted when creating innovations and ideas that define technical capabilities and products through which the development process of artifacts can be effectively and efficiently accomplished [Denning 1997; Hevner et al, 2004; Tsichritzis, 1998; Vaishnavi et al, 2004]. Design science research begins with awareness of the problem, real-world problem identification. The output could be a proposal. This is followed by the suggestion for a tentative design that is abductively drawn from the existing knowledge base for the identified problem area. The output is the tentative design. The next step is an attempt for artifact design which is derived from the suggested tentative solution(s), whereby

---

24 Artifact can be a model, a method, constructs, an instantiation or a framework: model is a set of propositions used to express a real-world problem and solution by the use of constructs; Constructs are concepts used for defining and communicating the identified problem and the proposed solutions; method refers to guidelines (steps) used to solve the identified problem by making use of constructs and/or models; and instantiation/instance refers to the implementation process of construct, framework, models, or methods [March & Smith, 1995].
development\textsuperscript{25} and evaluation\textsuperscript{26} is deductively performed. The design process is iterated back from the awareness, suggestion, development, to evaluation until the real-world situation is improved as indicated by the circumscription arrows shown in figure 2–2 below. Finally, conclusions (results) are drawn, indicating the completion of the design processes. The figure below depicts the general reasoning methodology in design science research.

![Diagram of Design Research Methodology](image)

*Figure 2–2: Design research methodology, compiled from Vaishnavi. & Kuechler [2004]*

Based on the above discussion, the goal of this research work was divided into four research studies along with their respective research questions, outlined in chapter 1.2. The research studies were linked into the design science research processes (steps) as follows:

- Study–1, RQ 1 was linked to awareness of the real-world problem step in DSR;
- Study–2, RQ 2 was linked to suggestions for a tentative design step in DSR;
- Study–3, RQ 3 was linked to developing the framework (artifact) step in DSR; and
- Study–4, RQ 4 was linked to evaluating the proposed framework step in DSR.

Additionally, because this research is dealing with security issues in e-government services, it was important to generate ideas on how to model the identified research problem as a system of systems. Therefore, systems–thinking\textsuperscript{27} concepts were adopted.

\textsuperscript{25} Development is the process of building or constructing artifacts (framework) [Hevner et al, 2004].

\textsuperscript{26} Evaluation is the process of assessing the output (performance measure) based on the defined criteria [Pierce, 1931].

\textsuperscript{27} Systems-thinking refers to the process of understanding how a set of objects together with relationships between the objects and between their attributes related to each other and to their environment so as to form a whole [Schoroderbeek et al, 1985,pp.12–100]; also, it is discussed in chapter 3.
[Schoderbeck et al., 1985]. Consequently, design science research was complemented in parts by systemic–holistic and socio–technical approaches such as soft systems methodology (SSM) [Checkland et al., 1990], systemic–holistic [Yngström, 1996] and socio–technical modelling [Kowalski, 1994].

Soft systems methodology (SSM) is a holistic approach for analysing complex situations in its real-world environment, and for proposing solutions to the identified problem. The approach is designed in such a way that it forms repetitive cycles of scientific inquiry. The methodology steps are: reflection step – refers to understanding of the complexity of the real-world problem area; planning step – refers to conducting extensive studies to explicitly understand the real-world problem; action step – refers to identifying, selecting and developing the best models and instruments for addressing the identified real-world problem; and observation step – refers to comparison and establishment of relationships between the knowledge-base and reality of the research problem. The process is repetitive until the real-world situation is improved [Checkland et al., 1990]. This methodology was used in research study–1, reported in research paper III; and in study–3, reported in research paper V. A detailed description for the systemic–holistic and the socio–technical approach are outlined in chapter 3. In addition, a description on how the approaches, including DSR, was applied in this research work is outlined in chapter 4, chapter 5, and also in Part II of this thesis.

2.3 Research Methods and Strategies

After identification of the most appropriate research approaches, the next step was to establish appropriate research methods (choices)\(^\text{28}\) and strategies that could be applied in this research work; they are depicted in layer three and four of GROP given in figure 2–1. Research methods are strategies for scientific inquiry that collects knowledge using defined procedures. It involves developing instruments for data collection, propositions, unit of analysis, and logic of linking data to the proposition [Saunders et al., 2003, Yin, 1994]. Basically, data can be collected through observation and/or measurement methods. The former refers to qualitative and the latter refers to quantitative research methods [Myers, 2009, Saunders et al., 2003].

To better understand these methods they are described as follows: Qualitative research method (QRM) is a field of scientific inquiry that crosscuts various disciplines and subject matters. Usually it uses qualitative data and involves in-depth interviews, observations and document reviews in order to understand human behaviour (social and cultural) and the entire situation [Creswell, 2003; Dawson, 2002;

\(^{28}\)Research methods (Choices) are categorized into Mono, mixed, and multi research methods. Mono-method refers to the use of single research method, either qualitative or quantitative, for data collection along with the associated data analysis technique. Mixed-method refers to the use of both research methods, qualitative and quantitative, for data collections along with the associated data analysis techniques. And Multi-method refers to the use of single research method, either qualitative or quantitative, for data collection along with the associated data analysis techniques (use of more than one research strategies) [Saunders et al., 2003].
Myers, 2009]. QRM requires small but focused samples and it often categorizes collected data into patterns as the primary basis for processing and analysing results. QRM reflects interpretive knowledge claims. It is often formative and non-generalizable. Examples of qualitative research methods include case-study\(^29\), survey-study\(^30\), action-research\(^31\), grounded-theory\(^32\), ethnography\(^33\), and archival-research\(^34\) [Myers, 2009; Saunders et al, 2003; Yin, 1994]. Contrary to qualitative research method, *quantitative research method (QtRM)* is a systematic scientific inquiry that uses quantitative data, numerical and/or statistical data. It involves studying the quantitative properties, phenomena and their relationships. QtRM reflects positivism knowledge claim, it is formative, and it is generalizable. Examples of quantitative research methods include survey, mathematical-modelling\(^35\) and laboratory experiments\(^36\) [Myers, 2009; Royer et al, 1999; Saunders et al, 2003; Yin, 1994].

Based on the nature of this research work, research studies and the corresponding research questions whose aim is to contribute to the research goal, a *qualitative research method* was chosen to guide this research work. Additionally, to ensure better research results when applying the selected research method, *research strategies* that are associated with qualitative research methods were adopted and applied. The selected research strategies were case-study, survey-study, and action research.

Consequently, research studies and their corresponding research questions that were linked to the DSR process (steps), outlined in chapter 2.2, were connected to research methods and strategies as follows:

- **Study–1**, RQ 1 linked to awareness of the real-world problem step in DSR. Case-study and survey research strategies were applied;
- **Study–2**, RQ 2 linked to suggestions for a tentative design step in DSR. Survey study research strategy was applied;
- **Study–3**, RQ 3 linked to developing the framework step in DSR. Action research strategy was applied; and
- **Study–4**, RQ 4 linked to evaluating the proposed framework step in DSR. Case-study and survey research strategies were applied.

\(^{29}\) Case-study is an empirical inquiry that investigates a phenomenon within its real context especially when the boundary between phenomenon and context are not clearly evident; it relies much on multiple sources of evidence [Yin, 1994].

\(^{30}\) Survey-research involves capturing data from individuals/groups using predefined structured questionnaires [Yin, 1994].

\(^{31}\) Action-research involves action and research; it can take positivist, interpretive or critical views. A critical view assumes that social and cultural reality is produced and reproduced by people [Myers, 2009].

\(^{32}\) Grounded-theory is an approach used for systematic discovery of new concepts and theories that are firmly grounded from empirical data; it is mostly applied for studying regular and repeated processes. [Myers, 2009].

\(^{33}\) Ethnography is a research design that enables researcher to explore and understands broader context of cultural phenomena which reflect the knowledge [Myers, 2009].

\(^{34}\) Archival-research is an approach that involves studying of existing data, including statistical records, survey archives, and written records. Archived data could be in the form of hard or electronic copies [Myers, 2009; Saunders et al, 2003].

\(^{35}\) Mathematical modeling refers to the description of systems using mathematical concepts and languages [Kothari, 2004].

\(^{36}\) Laboratory experiments are conducted in the environment that experimental variables are controlled [Kothari, 2004].
Detailed description for the research activities performed in each of the research studies, including the development of data collection instruments, are outlined in chapter 2.5 and summarized in table 2–6. In the next section, an outline of the research sample selections to be used for the empirical studies is presented.

2.4 Research Sample Selection

Given the fact that the real-world environment is vast, it was important to conduct research sample selections that would represent the real-world environment. Research samples were targeted for access to empirical studies [Jacobs et al, 1992; Myers, 2009; Yin, 1994]. The study environment of this research work was within the developing regions, where Tanzania was selected due to the following reasons: Tanzania is one of the developing countries located in Eastern Africa; it is still in her infancy stages of e-government services, implementation and service delivery; there has been scarcely few conducted research in the area, in particular in IT security, e-government, and eGMMs; there exists a number of security issues and challenges in relation to secure e-government services; and the author of this thesis is from the selected study environment.

Further, as this research work is conducted within Tanzanian environment, it was necessary to select a research sample (organizations) that would allow access for empirical studies. By the time when this research work activities were initiated (2009), Tanzania had approximately 21 ministries (M), 15 departments (D), and more than 17 agencies (A). These organisations are abbreviated as MDA. On selection of research sample the criteria were: only government organizations with a wide national coverage, and with a fairly high level of e-government services deployment and use; and organizations that offer e-government services which have direct impact on the national economy. Other criteria that had to be met were: organisations that have started implementing security services for securing e-government services, and organizations that would allow easy access to perform empirical studies. Based on these criteria, more than 20 MDAs (organisations) were contacted, out of which 6 organizations that met the set criteria were selected. The selected organisations were:

- **Organisation U** – a ministry responsible for managing the overall revenue, expenditure and financing of the government. It provides advice on financial affairs in support of the governments objectives in social and economic affairs, and prepares and presents the national budget. The ministry has a well-functioning IT directorate. It has about 90 IT personnel out of 1,100 personnel located country wide;

- **Organisation V** – a ministry that has a mandate to effectively administer land and human settlement development services in the country. Through the use of ICT (e-government), several issues and queries can be received and responded on-line.

---

37 Organizations names are kept anonymous due to ethical issues considerations [Myers, 2009]; they are discussed in chapter 2.6.
The ministry has an ICT directorate supported by 56 IT staff, where 16 are located at headquarter and about 40 are located country-wide. The ministry has a total work force of about 950 personnel;

- **Organisation W** – a ministry under the President’s office responsible for administration of public sector in the country. The organization structure includes a unit responsible for coordinating e-government initiatives country-wide. The unit has now (2012) effectively been promoted to e-Government Agency (eGA). The ministry has a total work force of about 290 personnel located country wide, of which 15 are being responsible for IT-related activities;

- **Organisation X** – a ministry under the Prime minister’s office in charge of providing good governance at all levels of regional secretariats (RSs) and local government authorities (LGAs) within the country. Currently, there are about 21 regions and 133 LGAs. The ministry has a directorate of management of information system (MIS). The directorate has about 6 IT staff located at the headquarter. They are assisted by one IT personnel located at each RS. The ministry has a total work force of about 246 personnel located country wide;

- **Organisation Y** – an agency in charge of managing all ports and cargo in the country. It is acting under the supervision of the ministry of infrastructure development. The agency has a well-established ICT directorate with about 34 IT personnel. The ministry has a total work force of about 3,500 personnel. It is now undergoing a major upgrading of the network infrastructure to effectively and efficiently support e-government services; and

- **Organisation Z** – an agency responsible for managing the assessment, collection and accounting of all central government revenues. It is operating under the supervision of the ministry of finance and economic affairs. It has an IT directorate of about 40 personnel. Currently the work force is about 3,000 personnel located country-wide.

The table below depicts estimated number of IT personnel and overall work force for each of the selected organizations.

*Table 2–2: Summary of IT personnel and overall work force in the selected organizations*

<table>
<thead>
<tr>
<th>Group Description</th>
<th>Organisation Name</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of IT personnel in the organisation</td>
<td>90</td>
<td>56</td>
<td>15</td>
<td>27</td>
<td>34</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Overall work force in the organisation</td>
<td>1,100</td>
<td>950</td>
<td>290</td>
<td>246</td>
<td>3,500</td>
<td>3,000</td>
<td></td>
</tr>
</tbody>
</table>

More details about the selected organisations are outlined in chapter 2.5, and research papers I, IV and VI [Karokola et al, 2009a, 2011a, 2012b].
2.5 Research Data Collection, Processing and Analysis Techniques

After identification and selection of suitable research approaches, methods and strategies, and a research sample of organizations that met a number of criteria, it was time for developing data collection instruments that would facilitate data collection undertaking. Indeed, the best research results could be achieved by selecting the best data collection techniques [Myers, 2009; Royer et al, 1999; Saunders et al, 2003].

To explicitly develop suitable instruments for data collection, processing, analysis and reporting, the following basic steps were followed [Kothari, 2004]: formulating the objectives of each study, designing the suitable technique for data collection, collecting suitable data, processing and analysing the collected data, and reporting the research results. What follows are the short descriptions on how these steps were performed:

- **Formulating the objectives of each study**: the goal of the research work was to propose a framework that would facilitate government organisations to effectively offer appropriate secure e-government services. To fulfil the research goal, four research studies with their respective research questions were formulated. Each of the research studies and questions were contributing to the research goal, see chapter 1.2. Basically, study–1 aimed at identifying and establishing the magnitude of the real-world problem, and also to creating awareness of the problem. Study–2 aimed at suggesting a tentative design of a solution/s that will mitigate the identified real-world problem. Study–3 aimed at developing a framework (artifact) for the identified real-world problem. And finally, study–4 aimed at evaluating the proposed framework. Detailed description on how the research goal was formulated, together with corresponding research studies and their respective research questions are outlined in chapter 1. Also, they are summarised in the subsequent sections.

- **Designing the suitable technique for data collection**: questionnaires, physical observations and interview schedules were designed to be the main sources of data collection from the studied organizations. Sources of evidence used in this research work were documentation such as ICT/IT security policies and strategies; case-studies and survey studies; in-depth interviews that include structured\(^{38}\) semi-structured\(^{39}\), and un-structured\(^{40}\) interviews; physical observation that included cultural artifacts; and in some cases, the use of audio recordings [Marshall et al, 1989; Myers, 2009; Yin, 1994]. Some of the developed and applied instruments are given in Annex D, E and F. After the design of the

---

\(^{38}\) Structured interview is the use of pre-formulated questions, strictly regulated by the order of the questions, and sometimes by the time availability [Myers, 2009, p.124].

\(^{39}\) Semi-structured interview is the use of some pre-formulated questions, but no strictly adherence to them; new questions might emerge during the conversion [Myers, 2009, p.124].

\(^{40}\) Un-structured interview is the use of pre-formulated questions, interviewees has free rein to say what they want. Often no set time limit [Myers, 2009, p.124].
suitable data collection instruments was completed, pilot studies were conducted in the selected organisations before the actual data collection was undertaken. The pilot studies consisted of selecting a few personnel within each of the selected organizations. After the completion of each of the pilot studies, the data collection instruments were further improved. Detailed descriptions of the activities performed in each study are given in the subsequent sections.

- **Collecting suitable data**: the improved versions of the data collection instruments, some examples are given in Annex D, E and F, were applied to the larger sample of the targeted personnel (professionals and experts) within the organisations for the actual data collection. The contacted groups within the organisations were at the strategic level: IT directors and decision and policy-makers; tactical level: IT managers and senior IT personnel; and operational level: IT technical personnel. The three stratified groups were chosen because they were key actors, either in decision making, planning, developing, implementing, maintaining and/or in delivering e-government services and security services. Additionally, considerable effort was used to ensure that reasonably large samples were drawn at the group level. In totality, the research took more than three years to complete. Therefore a time horizon for this research study was longitudinal. Detailed descriptions of the activities performed in each study are given in the subsequent sections.

- **Processing and analysing the collected data**: based on the nature of the research studies various techniques were cautiously applied for processing and analysing descriptive, analytical and statistical data. The techniques were used for examining, coding, categorizing, classifying, tabulating, and addressing initial propositions of study. In some cases they were used as a combination of both [Myers, 2009; Yin, 1994]. The content analysis technique was used for processing and analysing descriptive data. The technique looks for structures and patterns within the descriptive text. Further, it involves developing sets of categories of words and phrases, and codes them to a unit of text from which meaningful results are drawn [Myers, 2009; Pyne et al, 2004]. Similarly, the Microsoft Excel program was used as a tool for processing and analysing analytical and simple statistical data. Further, to ensure reliability, suitability and trustworthiness of the research results, before reporting it – triangulation and member-check.

---

41 Pilot studies were meant for testing easiness and processes for using the data collection instruments, getting feedback on the clarity of the instruments, and developing preliminary overview on the possible answers [Myers, 2009].

42 Professionals refer to personnel with working experience in the area of IT security and/or e-government of less than 10 years; whilst Experts refer to personnel with working experience in the area of IT security and/or e-government of 10 years and above.

43 Time-horizons refers to time required to conduct a study either longitudinal or cross-sectional. Longitudinal refers to when a particular study takes place over period of time; whilst cross-sectional refers to a study of a particular phenomenon at a particular point in time [Saunders et al, 2003].

44 Data processing refers to editing, coding, classifying, and/or tabulating the collected data in such a way that they are amenable for analysis [Kothari, 2004, p.122].

45 Triangulation technique refers to use of different methods that are pitted against one another in order to cross-check or validate data and its interpretations, it involves use of convergence of multiple data sources [Denzin, 1978].
techniques were applied. Detailed descriptions of the activities performed in each study are given in the subsequent sections.

- **Reporting the research results:** findings from each of the four main research studies were reported in seven research papers published in peer-reviewed internationally recognised professional and academic conferences and journals in information security and e-government. Also, the findings are summarised in *chapter 4*. The research papers were published as follows: findings from study–1 were reported in research *papers I, II and III*. Findings of study–2 were reported in research *paper IV*. Findings of study–3 were reported in research *paper V*, and findings of study–4 were reported in research *papers VI and VII*. The extended summaries of the research papers are presented in chapter 5, and full research papers are presented in Part II of this thesis.

Therefore, based on the general reasoning methodology in design science research (DSR), complemented in parts by the aforementioned systemic-holistic and socio-technical approaches, the research studies are summarized in figure 2–3 below. The figure outlines categorization and inter-dependencies between research studies, corresponding research questions and published research papers. Further, table 2–6 contains the summary of the same studies. Additionally, the table includes applied research methods and strategies, linkages of DSR steps, and the study environment where the research activities took place.

---

46 Member-checks technique refers to the process of cross-checking the pre-final research results with the respondents (source group) before casting it into final research results. [Denzin, 1978].
What follows are the detailed descriptions of research activities and processes performed at each of the research studies:

2.5.1 Study–1: Awareness of the Real-world Problem – Data Collection and Analysis

The aim of study–1 was to identify the real-world problem and to create an awareness of the problem. As a result sub-research questions RQ 1(a) and 1(b) was formulated. To address these sub-research questions, RQ 1(a) involved conducting extensive literature review and case-studies on various issues related to secure e-government services, implementation and service delivery, as well as issues related to secure e-government adoption in the real-world environment. The research results were reported in research papers I and II. One of the findings shows that eGMMs are used for guiding and benchmarking e-government implementation and service delivery in the target environment. Also, it was learnt that the model appears to lack security services, technical and non-technical, in their maturity stages. Consequently, leading to misalignment of the strategic objectives between e-government services and security services; resulting in in-secure e-government services. Therefore, the author was interested in addressing one of the cited security issues, particularly the lack of security services in the currently used eGMM. As a result RQ 1(b) was formulated. The RQ 1(b) involved extensive literature review and analysis of various eGMMs for security services. Based on the set of criteria, given in research paper III, eleven internationally recognised eGMMs were selected. Further, based on the set of evaluation criteria, given in Annex D–4, the selected models were extensively analysed for security services. The findings showed that all models lack security services, technical as well as non-technical. Also, the findings show that the models were structured differently within their maturity stages. Structural models were synthesized, whereby five maturity stages were developed, in order to propose a common frame of reference for eGMMs. The studies were conducted in April, 2009 and in early 2011. The findings from these studies, RQ 1(a) and RQ 1(b), were reported in research paper I and II, and paper III respectively. Also, the findings are summarised in chapter 4.

Questionnaire preparation process: a set of questionnaires were prepared, aimed at gathering important information on various issues related to secure e-government services as well as issues related to secure e-government adoption. The questions in the questionnaires were ranging from ICT/IT security and e-government policies; strategies, procedures, and awareness; assessment, auditing and monitoring; to factors affecting secure e-government adoption. Further, to test consistency and validity of the questionnaires a pilot study was conducted prior to exposing it to the personnel working in the government organization, identified earlier in chapter 2.4 [Karokola et al, 2009a]. The pilot study targeted only a few of the personnel: three personnel from each organization, one from each of the organizational levels. The pilot study was conducted via email communication. Responses from all respondents (N= 18) were received, and necessary improvements to the questionnaire were made. A sample of the developed and applied questionnaires is given in Annex D of this thesis.
**Questionnaire distribution and data collection process:** The improved versions of the questionnaires were distributed manually to the targeted personnel, 72 respondents, within the organizations (U – Z) as depicted in table 2–3 below. In the process, face to face interviews were also conducted, in particular when seeking clarification on some issues. And in some cases copies of documents related to ICT/IT security and e-government-related issues were collected as secondary data. The data collection process took about three weeks. A total of 51 completed questionnaires were collected (response rate= 70.8%). The table below shows the matrix for the contacted and responded personnel within the studied organizations.

**Table 2–3: Study–1. Number of respondents in the researched organizations**

<table>
<thead>
<tr>
<th>Organization Names</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>4</td>
</tr>
<tr>
<td>V</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>W</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>X</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Y</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Z</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Total</td>
<td><strong>12</strong></td>
<td><strong>24</strong></td>
</tr>
<tr>
<td></td>
<td><strong>72</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Data processing and analysis:** Collected data were cautiously processed and analysed. Data were categorized into descriptive and analytical/statistical data. When processing and analysing descriptive data, content analysis was used. When processing and analysing analytical and simple statistical data the Microsoft Excel tool was used. Further, to ensure reliability, suitability and trustworthiness of the research results, before reporting it triangulation and member-check techniques were applied. For instance, triangulation technique was applied for cross-checking the reliability, suitability and trustworthiness of primary-data47 and its interpretation by comparing it with secondary-data48. Member-check technique was applied for cross-checking the reliability, suitability and trustworthiness of the research findings before reporting the final research result. The process involved the cooperation of some personnel in the studied organisations.

47 Primary–data, in this thesis, refers to data that was collected, in the studied environments, based on the developed data collection instruments (i.e. questionnaires) [Myers, 2009].

48 Secondary–data, in this thesis, refers to additional data that was collected in the studied environments, such as ICT/IT policy documents and audio recordings [Myers, 2009].
2.5.2 Study–2: Suggestions for a Tentative Design – Data Collection and Analysis

The aim of study–2 was to identify and propose the possible security measures that would address the identified security problem in the real-world environment, lack of security services in eGMMs stages, addressed in RQ 1(b) and research paper III. As a result, research question RQ 2 was formulated. The study involved conducting an extensive literature review on various information security maturity models, standards, and best practices. Some are presented in chapter 3, whereby information security maturity models (ISMMs) appeared to be more appealing. This is because the ISMMs security services are designed in a continuous incremental order from the lower to highest critical maturity levels, likewise for e-government services in eGMMs stages. Consequently, based on the set criteria, defined in research paper IV, eight internationally recognised ISMMs were selected and extensively analysed for security services enhancement, technical and non-technical. Further, models with orientation towards security awareness, evaluation and management were then synthesised and five critical maturity levels were proposed. To affirm the findings a survey study was conducted in the previously studied organizations (U – Z). The selection criteria for the survey study as a strategy for data collection were based on the nature of the study and time limitation. The study was conducted in March, 2011. The findings from this study were reported in research paper IV. Also, the findings are summarised in chapter 4.

Questionnaire preparation process: questionnaires were prepared, aimed at gathering stakeholders’ views on the proposed ISMM critical levels and their respective security services requirements control areas, technical and non-technical. To be able to comprehensively establish security service requirements control areas, it was important to identify key security requirement areas. So, security services requirements control areas (technical and non-technical) from the Security-By-Consensus model (SBC) [Kowalski, 1994] were adopted. In addition, an awareness programme was added as part of the non-technical security control area [Henry, 2004; Karokola et al, 2009a, 2010]. To test consistency and validity of the questionnaire, another pilot study was conducted in the previously studied organizations. The pilot study was conducted via email communication [Karokola et al, 2011a]. This pilot study targeted one respondent from each organization (N= 6). Responses from all targeted respondents were received, and the required improvements to the questionnaire were made. A sample of the developed and applied questionnaire is presented in Annex E–2, tables E–1 and E–2 of this thesis.

Questionnaire distribution and data collection process: an improved version of the questionnaire was re-distributed via email to the selected respondents (N= 18), within the organizations as depicted in table 2–4 below. Due to time constraints respondents were given only one week to respond. After expiration of that period, a follow-up to collect the completed questionnaires, using telephone and email, was made. A total of 13 completed questionnaires were collected (response rate= 72.2%). Table 2–4 below shows the number of contacted and responded personnel in the surveyed organizations.
Table 2–4: Study–2. Number of respondents in the researched organizations

<table>
<thead>
<tr>
<th>Organization Names</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>1</td>
<td>1</td>
</tr>
<tr>
<td>V</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>W</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>X</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Y</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Z</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

Data processing and analysis: collected data were cautiously processed and analysed. The analysis process was categorized into descriptive and analytical data. For processing and analysing descriptive data content analysis technique was used. When processing and analysing analytical data the Microsoft Excel tool was used. In addition, categorization of the research results was based on the stratified groups in the organizations (strategic, tactical and operational levels). The research results affirmed the proposed five ISMM critical levels. Thus, the proposed ISMM levels together with their corresponding security service requirements control areas were confirmed by the respondents.

2.5.3 Study–3: Developing the Framework – Data Collection and Analysis

The aim of study–3 was to develop a framework that would appropriately integrate the identified ISMM security service requirements control areas (addressed in RQ 2, paper IV) into the maturity stages of eGMMs (addressed in RQ 1(b), paper III) for securing e-government services. As a result, research question RQ 3 was formulated. As this study had to do with developing a catalogue of security services requirements control areas for the proposed framework, it was important to involve respondents who were more knowledgeable regarding technical and non-technical security aspects. Therefore, a group of PhD and Master students in information and communication systems security (ICSS) from the department of computer and systems sciences (DSV), Stockholm University/ Royal institute of technology (KTH) in Sweden, was selected for the undertaking. The study was conducted in April, 2011 in Stockholm, Sweden. The findings from this study were reported in research paper V. Also, the findings are summarised in chapter 4.

Questionnaire preparation process: questionnaires were prepared with focus on obtaining a comprehensive matching of a security services requirements control areas (SRCAs) catalogue, which is based on the proposed five critical maturity levels of
ISMMs [Karokola et al, 2011a]. After conducting an extensive literature review on existing security models, standards and best practices, security services requirements control areas (technical and non-technical) were identified and selected. These included the twelve security control principles adopted from the ISO-27002, which are summarised in Annex E–3 table E–3. It also included the information security management maturity model, summarised in Annex E–3 table E–4; as well as the Common criteria, summarised in Annex E–3 table E–5; and the Systems security engineering capability maturity model, summarised in Annex E–3 table E–6. These Annexes are given in Part III of this thesis. Thus the development of SRCAs catalogue was divided into three processes:

- Matching the SRCAs from tables E–4, E–5, and E–6 to their corresponding ISO–27K security control principle elements, listed in table E–3;
- Matching the SRCAs developed in table E–3 into table E–7. Table E–7 has five ISMM levels (proposed in study–2, research paper IV), which were categorized into three major types of security service requirements control areas (SRCAs): security objectives, security processes, and security metrics. Furthermore, each of the SRCAs was categorised into technical and non-technical security aspects; and
- Matching the SRCAs from those matched in table E–7 into tables E–8 and E–9. These tables were intended for a thorough analysis of the SRCAs for the lowest and highest critical maturity levels of ISMM respectively (described in study–2 research paper IV and study–3 research paper V).

To test the questionnaire another pilot study was conducted, involving two selected experts in the area and two PhD students, from DSV, Stockholm University, Sweden. Comments from all respondents were received and the necessary improvements of the questionnaire were made. A sample of the developed and applied questionnaires is given in Annex E–3 of this thesis.

**Questionnaire distribution and data collection process:** A final version of the questionnaires was physically re-distributed to the 48 ICSS students at DSV, Sweden, 43 Master and 5 PhD students, for matching and developing a catalogue of security services requirements control areas, as described earlier. Before filling in the questionnaire, explanation on the purpose of the study and on how to respond, were given to the respondents. Also, the respondents were able to ask for clarification before and during the undertaking. At the end of the Masters students session 31 questionnaires out of 43 were completed and collected. The remaining questionnaires (12 of the 43) were completed and collected within one week. The data collection process for the 5 PhD students was done separately. All five questionnaires were completed and collected. In total, all 48 questionnaires were completed and collected (response rate = 100%).

---

49 Definitions about security objectives, security processes and security metrics are given in the footnote of chapter 4.1, sub-step–3.4
Data processing and analysis: all collected data were cautiously processed and analysed. The data was categorized into descriptive or analytical data. For processing and analysing descriptive data, a content analysis technique was used. For analysing analytical data, the Microsoft Excel tool was used. Results were categorized based on the proposed ISMM critical levels and their corresponding SRCAs areas. Detailed information on the developed catalogue of SRCAs is given in Annex C. Furthermore, based on these findings a pictorial view of a framework for securing e-government services which integrates IT security services into eGMMs was developed.

2.5.4 Study–4: Evaluating the Framework – Data Collection and Analysis

The aim of study–4 was to evaluate the proposed framework “a framework for securing e-government services which integrates IT security services into eGMMs” developed in RQ 3 reported in paper V. As a result, research question RQ 4 was formulated. The study was conducted in six government organisations studied earlier. The evaluation process aimed at rigorously providing essential feedback to the building and development processes by demonstrating utility\(^{50}\), quality, and efficacy of the proposed framework [Guba, 1981; Hevner et al, 2004; Zelkowitz et al, 1998].

Evaluation methods could be either practical, theoretical or both. Practical evaluation methods include 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 [Denzin, 1978; Guba, 1981; Hevner et al, 2004; Kothari, 2004; Zelkowitz et al, 1998]. 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. However, the methods appear to have poor control of the results for later replication [Denzin, 1978; Guba, 1981; Hevner et al, 2004; Zelkowitz et al, 1998].

Based on the above analysis, practical evaluation approaches require implementing the framework to the real-world environment. Possibly 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 in the same organisations studied earlier in Tanzania. The study was conducted in May, 2012. The

---

\(^{50}\) Utility refers to usefulness of the IT artifact; efficacy refers to artifact ability to produce the desired effect; and quality can be demonstrated by evaluating the artifact in terms of functionality, performance, reliability, usability and completeness [Hevner, 2004].
findings from this study were reported in research paper VI. Also, the findings are summarised in chapter 4.

**Questionnaire preparation and testing process:** questionnaires were prepared aimed at evaluating the proposed framework. To be able to comprehensively evaluate the framework, it was important to identify and develop suitable evaluation criteria. Based on the existing literature [Davis, 1989; Guba, 1981; Hevner et al, 2004; Venkatesh et al, 2008; Zelkowitz et al, 1998] seven framework evaluation criteria were formulated. The formulated criteria were: *simplicity, coverage and completeness, compliance to security standards, and dynamics and flexibility.* Other criteria were: *capability and relevance, usefulness, and trustworthiness.* For details, see Annex F of this thesis. When conducting a case study, a semi-structured interview was administered. The approach involved the use of pre-formulated questions (some) with provision for opinion/ comments and new questions were emerging during the interview process [Myers, 2009]. In order to test consistency and validity of the questionnaire, another pilot study was conducted in the earlier studied organizations. Pilot study was conducted via email communication. The pilot study targeted a few selected respondents, one personnel from each of the six organization located in Tanzania (N= 6) and two experts from the academia, DSV/Stockholm University, in Sweden. After receiving answers from all respondents, necessary improvements of the questionnaire were made. A Likert scale was employed when rating the framework acceptability evaluation criteria [Kothari, 2004]. The scale ratings were: *strongly disagree, disagree, not sure, agree,* and *strongly agree.* Furthermore, space for the respondents to give their opinion was provided within the same questionnaires. A sample of the developed and applied questionnaire is provided as part of this thesis in Annex F of this thesis.

**Questionnaire distribution and data collection process:** a total of 90 copies of the improved version of the questionnaire were physically re-distributed to the earlier studied government organizations located in Tanzania. In the process of conducting the data collection undertaking, respondents were briefed on the aim of the study, and also on how the proposed framework works. Also, this information was provided in the Annex of the questionnaire. A total of 69 (response rate= 76.7%) filled questionnaires were collected from the surveyed organisations. Data collection process took two weeks. Table 2–5 below shows the number of the contacted and responded personnel within the studied organisations.
Table 2–5: Study–4. Number of respondents in the researched organizations

<table>
<thead>
<tr>
<th>Organization Names</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><strong>Total</strong></td>
<td><strong>12</strong></td>
<td><strong>36</strong></td>
</tr>
</tbody>
</table>

**Data processing and analysis:** collected data were cautiously processed and analysed. The data was categorized into descriptive and analytical data. For processing and analysing descriptive data content analysis technique was used. When processing and analysing analytical/simple statistical data the Microsoft Excel tool was used. Further, the analysis was divided into three major parts: the first part analyses the frequency of acceptability, organisational-wise, for the proposed framework. The second part gives the comparative analysis on the degree of the framework acceptability among the stratified groups: strategic, tactical and operational levels. The third part addresses the areas of framework improvements, which is based on the respondents’ opinions.

2.6 Ethical Issues Considerations

Ethics is an important issue when conducting research [Myers, 2009; Yin, 1994]. This research work was guided by the practical principles cited by Myers [2009, pp. 45 – 51]. Plagiarism was avoided by acknowledging all used sources by referencing. Also, confidentiality of the collected data from the studied organizations was ensured by providing anonymity to sources of information, including coding of organization names, when necessary, as shown in chapter 2.4. Further, research biasness was avoided during the data collection, processing and analysis, and reporting the final research results by applying rigorously research methods including the use of triangulation and member-checks techniques. In addition, the research complied with the laws of the countries where the studies was conducted, such as seeking permission before conducting an interview in any of the targeted organizations. Annex D–1, E–1, and F–1 shows a sample of introductory letters used when the research studies were conducted.
2.7 Chapter Summary

This chapter presented the analysis of the problem of securing e-government services in the real-world environment. The study was interpretative, inductive, qualitative, explorative, and descriptive in nature. Also, the study was longitudinal, since it took more than three years. The study applied concepts from a number of rigor research approaches, methods, strategies and techniques as summarized in figure 2–4 below. The figure is an extension of figure 2–1 given at the beginning of this chapter, whereby the applied research areas are shaded (from the research philosophical assumptions to data collection and analysis techniques).

Additionally, the research study was mainly guided by a design science research (DSR) approach complemented in parts by systemic-holistic and socio-technical approaches, discussed in chapter 3. The table below is an extended version of table 1–1 given in chapter 1, whereby the applied, research methods and strategies, DSR steps, and the study environment where the research activities took place are mapped against the corresponding research studies, questions and published research papers.
Table 2–6: Extended table for research studies, questions, papers, and applied methods and strategies

<table>
<thead>
<tr>
<th>Research study</th>
<th>Research RQ</th>
<th>Papers</th>
<th>Applied research methods and strategies</th>
<th>DSR steps</th>
<th>Study environment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>QRM</td>
<td>QtRM</td>
<td>Case-study</td>
</tr>
<tr>
<td>1</td>
<td>1(a)</td>
<td>I</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>1</td>
<td>1(b)</td>
<td>II</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>1</td>
<td>1(b)</td>
<td>III</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>IV</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>V</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>VI</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>VII</td>
<td>√</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The next chapter outlines an overview of the theoretical foundation for modelling e-government maturity models (eGMMs), e-government services, and security services.
3. Theoretical Foundation for Modelling e-Government Services

The previous chapter, chapter 2, established the research methodology for this research work. This research work is guided by a design science research, complemented in part by systemic-holistic and socio-technical approaches. In this chapter, the theoretical foundation for modelling IT security services into e-government maturity models for achieving secure e-government services is presented. The theoretical foundation is used to guide the studies on deciding what effective and appropriate approaches should be used to achieve the research goal.

The chapter is organised as follows: it starts by outlining the descriptions for understanding the internationally recognised e-government maturity models and problem areas, followed by understanding of IT security related terminologies and their inter-relationships. This is followed by introducing the concepts on systems-thinking, including how to holistically investigate, learn, and model the IT security problem area. Lastly, concepts on understanding mitigation measures for IT security problem area and chapter summary are presented. Figure 3–1 below shows the chapter sections flow.

![Figure 3–1: Theoretical foundation sections inter-relationships](image)

3.1 Understanding e-Government Maturity Models and the Problem Area

The central problem area that the goal of this research work is addressing is the lack of security services, technical and non-technical, in e-government maturity models. The section presents an overview of internationally recognised e-government maturity models along with their analysis for security services.

e-Government maturity models (eGMMs) are models where the design and development process is based on the concepts from the capability maturity model
These models were developed by international organizations, consulting firms, academia and individual researchers specifically for guiding and benchmarking e-government implementation and service delivery in a stage-wise approach [Karokola et al., 2012a]. eGMMs define different maturity stages. A maturity stage reflects the level of e-government maturity, degree of technology complexity, degree of systems sophistication, and level of interaction with users [Gronlund et al., 2005; Moon, 2002; WorldBank, 2001, 2003]. The advantage of having a stage-wise approach in eGMMs is to offer governments the ability to measure the progress of e-government implementation and service delivery, giving them flexibility to develop and prioritize e-government-related activities, and facilitating organizations to meet their e-government goals by ensuring that business and technological components are effectively aligned [Gronlund et al., 2005; Iran et al., 2006; Layne et al., 2001; UN, 2008; WorldBank, 2003].

However, being effectively aligned does not mean being secured. In this regard, offering secure e-government services appeared to be a major challenge due to absence of effective security approaches that would appropriately mitigate security risks and threats posed to e-government services. This calls for extensive investigation of the models’ security services, strengths and weaknesses. Consequently, a comparative analysis of eleven internationally recognised eGMMs for security services was conducted. The results showed that eGMMs lack built-in security services (technical and non-technical) within their maturity stages [Karokola et al., 2012a]. A comprehensive list of eGMMs along with analyses for structural design and security services is outlined in research paper III [Karokola et al., 2012a]. Thus, to explicitly address security services requirements in eGMMs – better understanding of theoretical foundations to information security is necessary. Therefore, the succeeding sections were introduced.

3.2 Understanding Information Security Terminologies and their Relationships

To adequately address the problem of lack of security services in e-government maturity models, in relation to the goal of this research work, understanding of the information security terminology and their relationship, is important. This section briefly presents general concepts for IT security terms: security risks, security threats and security vulnerabilities in relation to e-government services.

Security risk refers to the potential that given threats would exploit vulnerabilities of e-government systems, and consequently cause harm to the organization information assets. Security risks affect confidentiality, integrity and availability (CIA) of e-government information assets while being processed, transmitted and stored across e-government domains. Security risks could be measured in terms of a combination of the probability of an event to occur and its consequence [ISO-27k, 2008; NIST, 2002, 2007a].
Security threats refer to any circumstance or event with the potential to adversely impact organizations critical assets, through un-authorized access, destruction, disclosure, or modification of information assets [ISO-27k, 2008]. Security threats exploit specific vulnerabilities within e-government systems and applications; hence, affecting confidentiality, integrity and availability of critical information assets [NIST, 2008]. According to NIST [2002, p.13] common threat-sources could originate from human-made, natural calamities and/or the environment. Human threats comprises of events that are caused by human acts, either intentional or accidental. Intentional threats are attacks caused deliberately by human beings such as network based, malicious software, and unauthorised access to confidential information. Similarly, accidental threats are attacks that are not deliberate, such as a hardware failure [ISO-27k, 2008; NIST, 2002, 2007a]. All these types of security threats could potentially affect CIA of e-government services.

Security vulnerability refers to flaws or weaknesses in system security procedures, design, implementation, and/or internal controls that could be exploited by threat-sources. Once exploited it could result into a security breach, consequently causing harm to e-government information assets and services [NIST, 2002, p.15]. Figure 3–2 below shows the inter-relationship between the three security terms and how they relate to each other. The figure could be interpreted as follows:

- the Owner of the e-government information assets, government organisation, perceives security threats; security threats tend to exploit the vulnerability of e-government information assets; consequently, it gives rise to security risks of the e-government information assets; and
- depending on the likelihood of the threats being realized and the impact on e-government information assets when the threats are realized – the assets Owner would impose countermeasures to mitigate security risks to assets. Countermeasures may be of technical and/or non-technical security aspects.

Figure 3–2: Security concepts and their inter-relationships [CC, 2009, p.39]

51 Threat-sources refers to intentional or accidental sources of threats that may exploit vulnerabilities of a system [NIST, 2002]
Reducing any of the three elements, security threats, security vulnerabilities and impact, could result into a significant reduction of security risks. Understanding these information security terminologies and their inter-relationships gave basis for building the theoretical foundation on how to develop effective security measures that would appropriately mitigate security risks and threats posed to e-government services; hence achieve secure e-government services. Therefore, the succeeding sections were introduced.

3.3 Understanding the Concept of Systems–thinking and Holistic Approaches

This section outlines the description of systems-thinking and holistic approaches that could be applied for better understanding, investigating, and modelling IT security problem in e-government services. Developing an effective security service approach for mitigating security risks and threats posed to e-government services would result in government organisations offering more secure e-government services.

The General systems theory (GST) defines and investigates systems integrity, complexity and their phenomena free from any biasness, and what makes system a system [Yngström, 1996]. A system is “a set of objects together with relationships between the object and between their attributes that are related to each other and to their environment so as to form a whole” [Schoderbek et al, 1985, p.12]. The definition offers key elements for conceptual understanding of a system, and on how to model an IT security problem in e-government services, as a system of systems. The systems’ key elements are: a set of objects, relationships, attributes, environment, and a whole. To better understand the systems’ key elements, they are described below [Schoderbek et al, 1985, pp.12–26]:

(a) System’s objects: refers to the systems elements that make the said system meet its objectives. For the system to meet its objectives, its parts must perform their basic functions. The basic functional parts are: input (I), process (P), output (O) and feedback. Input refers to output from other systems or feedback from the same system. Process is the system transformation of input to output. Output refers to output that is to be input to other systems or to the system itself. Feedback refers to the mechanism of a system to control and communicate for the purpose of maintaining a balance of its internal structures;

(b) System’s relationships: refers to bonds that link system’s objects and/or sub-systems together. It creates unique inter-relationships between systems and between sub-systems;

(c) System’s attributes: refers to the properties of both objects and relationships. Attributes facilitates delimitation of the system from its operating environment. Also, it facilitates the ways by which important chains of relations and dependencies of systems are known, observed and/or introduced;
(d) **System’s environment:** refers to something outside the system, which the system cannot directly control. But the environment may in parts determine system’s performance. A system cannot control its environment but may influence its environment through its output; and

(e) **Whole/wholeness:** refers to all properties of a given system taken together. Wholeness cannot be determined by breaking up the system into sub-systems or parts.

A system can be **open** or **closed**. An **open system** refers to systems whose boundaries permit a flow of information in and out of the system. A **closed system** is the one whose boundaries do not allow a flow of information in or out of it. Figure 3–3 below depicts the concept of an open system with input (I), processes (P), output (O) and feedback.

![Figure 3–3: An open system within its environment](schoderbeketal1985p25)

The output from other systems becomes input to the system and the output of the system becomes input to other systems. Additionally, a system has a boundary that demarcates (isolates) it from its environment. Indeed, system boundaries show that there is interaction and exchange of information between the system and its environment. Further, within the system itself - not all output are going out of the system to influence its environment. Some may become an input or feedback within the same system. A feed-back mechanism plays an important role for control and communication in a system and depends on a requisite variety. This introduces us to the principles of control in cybernetic systems [Schoderbek et al, 1985].

These principles are useful for modelling the identified real-world security problem, lack of security services in eGMMs, which affects secure e-government
services. The principles for governing control functions in a cybernetic system are [Beer 1968, in Schoderbek et al, 1985, pp.109–112]:

- Control principle I: “*implicit controllers depend for their success on two vital tricks: the first is the continuous and automatic comparisons of some behavioural characteristic of the system against a standard; the second is the continuous and automatic feed-back of corrective actions*”; 
- Control principle II: “*in implicit governors, control is synonymous with communication; control is achieved as a result of transmission of information. to be in control is to communicate*”; and
- Control principle III: “*in implicit controllers, variables are brought back into control in the act of and by the act of going out of control*”.

To explicitly describe the control principles, the system boundary given in figure 3–3 is extracted, and the feedback system control mechanism is looked in high resolution (expanded) as depicted in figure 3–4 below.

![Figure 3–4: A control system, simplified [Schoderbek et al. 1985, p.104]](image)

The figure is described as follows [Schoderbek et al, 1985]:

- A detector is meant for detecting specified output variables of a given control objective, of which the values are sent to the comparator;
- A comparator, compares the actual values to the accepted variances and signals for the deviation are sent to the effector; and
- An effector decides which action is to be taken based on the deviation and feeds back this information to the system to be controlled. These signals are taken as new inputs.
In this regard, the outputs from the system to be controlled is checked and fed back as control information so as to change the system’s behaviour for the next cycle. These theoretical foundations, on systems-thinking, gave a basis for analysing the system of study in its real-world environment. Security services in e-government should be an integral part of e-government services from planning, designing, development, implementation, service delivery, to maintenance phases. This way feed back will be able to control security risks and threats posed to e-government services. Implying that, implementing security services into eGMMs could be the best approach towards achieving secure e-government services, because strategic goals for e-government services and security services would be appropriately aligned. Therefore, to appropriately model the identified security problem in eGMMs the following steps are followed:

Firstly, the real-world problem is mapped into figure 3–3 as follows:

- The system’s environment is mapped to includes citizens (C) and business (B);
- The system’s boundary is mapped to includes government organisations (G);
- Inside the system boundary there are the following: e-government services (applications and protocols infrastructure) and its supportive mechanisms such as eGMMs, e-government information assets, e-government and security policies mechanisms; and
- Technical and non-technical security risks and threats posed to e-government services may came from within or outside the system’s boundaries (the system’s environment).

Secondly, the above identified real-world environment is then mapped into figure 3–5 below. The figure is an extension of figure 3–3, which shows an open system with a mapped real-world environment into the system’s environment and boundary.

*Figure 3–5: Mapping of real-world environment into an open system*
Thirdly, to explicitly narrow the area of focus, the system’s boundary is explored by applying it into figure 3–4. Since inside the system’s boundary one of the critical elements is eGMMs, that appear to lack security services in the maturity stages (see research paper III), it is compared to a detector, a comparator, and an effector. Meaning that eGMMs should be modelled to include security services in such a way that it should be capable of:

- **detecting** security risks and threats posed to e-government services (modelling of security services objectives to mitigate technical and non-technical related security risks and threats);
- **comparing** the security risks and threats posed to e-government services for appropriate security services measures (measuring security services metrics to mitigate technical and non-technical related security risks and threats); and
- **effecting** the appropriate security services measures for mitigating such security risks and threats (managing security services processes to mitigate technical and non-technical related security risks and threats).

The questions on what elements and attributes that should be detected (modelled), compared (measured), and effected (managed) requires a deeper understanding of the real-world security problems. This calls for a systemic-holistic approach. Yngström [1996, p.27] proposed the systemic-holistic approach guiding principles (SHA GP–#) for handling security problems in the real-world environment, they are summarised in Table 3–1 below:

<table>
<thead>
<tr>
<th>SHA GP–#</th>
<th>Description of guiding principles (SHA GP–#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA GP–1</td>
<td>delimit the system of study from the environment</td>
</tr>
<tr>
<td>SHA GP–2</td>
<td>define the existing environment</td>
</tr>
<tr>
<td>SHA GP–3</td>
<td>define the in-flow, through-flow, and out-flow</td>
</tr>
<tr>
<td>SHA GP–4</td>
<td>structure the in-built control system so that it can deal with inner and outer variety</td>
</tr>
</tbody>
</table>

Fourthly, to explicitly follow these guiding principles (SHA GP–#) when addressing the existing IT security problem in eGMMs, the systemic-holistic approach [Yngström, 1996] and socio-technical modelling [Kowalski, 1994] was applied as follows:

To delimit the system of study from the environment (SHA GP–1) a systemic-holistic approach (SHA) was applied. SHA facilitates investigating and understanding security problems in relation to real-world environment free from any biasness. This way paradigm, values and other related security entities can explicitly be defined in its context and applicable environment [Yngström, 1996]. According to Yngström [1996] the model is organized into two parts, epistemology and framework. The

---

Epistemology is the fundamental theoretical aspects of knowledge, its proposition, methods, limitations and validation [Yngström, 1996].

---
epistemology part acts as a meta-disciplinary tool and criteria of control and communication. The framework part is organised into three dimensions: levels of abstraction, context orientation, and content subject area. Figure 3–6 below shows an overview of the systemic-holistic model.

![Figure 3–6: Overview of systemic-holistic model [Yngström, 1996, p.19]](image)

When scrutinizing the model further the following issues are of interest: different levels of abstraction have physical construction, theory and model, and design and architecture. Context orientation have geographical and time bound. The content/subject area has technical and non-technical security aspects. Further, the technical security aspects have process, store, communicate, collect and display; whilst non-technical security aspects has operational, administrative and managerial, legal and ethical security aspects [Yngström, 1996]. Figure 3–7 below depicts a detailed overview of the model dimensions.

![Figure 3–7: Detailed view of the systemic-holistic model [Yngström, 1996, p.20]](image)

In this research work, SHA was extensively applied in the preliminary studies aimed at gathering holistic understanding of the factors affecting secure e-government services, implementation and service delivery, in the real-world environment. The
holistic investigation applied the detailed part of the SHA framework, depicted in figure 3–7, covering a wide range of security related issues from technical to non-technical; for details see Annex D–2 and D–3. The research processes and results from this study are summarised in chapters 2.5.1 and 4 respectively. Additionally, research paper I shows the details on how the approach was applied, and the reported research results.

Furthermore, to be able to comprehensively model, the identified IT security problems, lack of security services in eGMMs, in relation to guiding principles (SHA GP–2 and SHA GP–3), socio-technical modelling was applied [Kowalski, 1994]. A socio-technical model deals with modelling multi-disciplinary inquiry of IT security problems [Kowalski, 1994]. At the abstract level, the model is divided into two sub-systems, social and technical. Within a given sub-system there are further sub-systems. The former (social) has culture and structures, and the latter (technical) has methods and machines, see figure 3–8 below.

From the system theory/s point of view, interdependencies between system levels makes a system adjust for attaining equilibrium. The process is referred to as homeostasis\textsuperscript{53} state. For instance, if new hardware is introduced into one of the technical sub-systems, let’s say the machine sub-system; the whole system will strive to achieve homeostasis. This suggests that changes in one sub-system may cause disturbances in other sub-systems and consequently to the entire system. Additionally, Kowalski [1994] proposed a detailed part of socio-technical model that shows how security can be modelled. The model is named as Security-By-Consensus (SBC), depicted in figure 3–9 below.

\textsuperscript{53} Homeostasis is the process of maintaining static or dynamic equilibrium between different and independent element of the system irrespective of external effects. OR maintaining the property of a system, either open or closed that regulates its internal environment and tends to maintain a stable constant condition [Schoderbek et al, 1985]
Basically, the SBC model is composed of two sub-systems, social and technical. The social sub-system is further divided into other sub-systems, ethical and cultural norms, legal and contractual documents, administrational and managerial policies, and operational and procedural guidelines. Similarly, the technical sub-system is divided into mechanical and electronic, hardware, operating systems, application systems, and data. Other aspects are: store, process, collect, and communication.

In this research work, the SBC model was first applied for clearly defining the existing system’s environment, eGMMs in its environment (SHA GP–2). In this case, based on the set of selection criteria defined in research paper III, internationally recognised eGMMs were extensively analysed for security services. The security services requirements evaluation criteria, technical and non-technical, were developed from the SBC model and the twelve security control principles extracted from the ISO-27002; for detail see Annex D–4. The research processes and results from this study are summarised in chapters 2.5.1 and 4 respectively. Additionally, research paper III shows the details on how the approach was applied, and the reported research results.

Further, the SBC model was applied for defining the in-flow, through-flow, and out-flow (SHA GP–3). In the process, based on the set selection criteria defined in research paper IV, internationally recognised information security maturity modes (ISMMs) were extensively analysed and synthesized for security services enhancement. Whereby, the in-flow, through-flow, and out-flow security service requirements were modelled and clearly defined in continuous order, called security maturity levels of ISMM; for detail see Annex E–2, tables E–1 and E–2. The research processes and results from this study are summarised in chapters 2.5.2 and 4 respectively. Additionally, research paper IV shows the details on how the approach was applied, and the reported research results.

Moreover, to appropriately structure the built-in control system in such a way that it can deal with inner and outer variety (SHA GP–4), effective security service measures were developed for the identified IT security problems in eGMMs. The developed security service measures in eGMMs were capable of appropriately detect, compare, and effect security service measures (security varieties) against security risks and threats posed to e-government services. This capability was achieved by strengthen the framework development processes by utilizing more knowledge from the GST, cybernetic principles and other security mitigation measures; for detail see chapter 3.4 and Annexes E–3 and F. The research processes and results from this study are summarised in chapters 2.5.3 and 2.5.4, and 4 respectively. Additionally, research papers V and VI shows the details on how the approach was applied, and the reported research results.
3.4 Understanding Mitigating Measures for IT Security Problem Area

This section is an extension of the previous one. It presents some of the security services mitigation measures used for developing the proposed framework for securing e-government services along with a catalogue of security service requirements. These results are also summarised in chapter 4, and detailed in research papers published in peer-reviewed internationally recognised conferences and journals in information security and e-government. Criteria for the selection of the mitigation measures including information security maturity models, standards and best practices are outlined below, and detailed in the respective research papers.

3.4.1 ISO/IEC 27000 Family: Code of Practice for Information Security Management

The ISO/IEC 27000 family is one of the most widely referred codes of practice for information security and management. It is based on ISO 17799. The ISO 27000 family provides standards for best practice guidelines on system design, information security management, and controls. It comprises of, at least the following: ISO 27001 covers information security management systems requirements certification standard/specification including standards for establishment, implementation, control and improvement of the information security management system (ISMS), ISO 27002 describes code of practice for information security management including a comprehensive set of information security controls. Its objectives and a set of generally accepted practice (ISO/IEC 17799 was last revised in 2005 and renamed as ISO/IEC 27002:2005). And the ISO 27005 was designed to give security advice on information risk management. The twelve guiding security control principles of the ISO/IEC 27002 are:

(i) Risk assessment and treatment: provides guiding principles on how to perform risk assessment and treatment. It includes systematic methods for assessing threats and vulnerabilities, and comparing assessed risks against established risk criteria;

(ii) Security policy: gives guidance and directives to the security management;

(iii) Organisation of information security: provides detailed description on how the internal security structures should be organised, and governance of information security;

(iv) Assets management: gives ways and best approach on inventory and classification of information assets;

(v) Human resource security: provides directives on security issues for employees who are joining and/or leaving the organisation;

(vi) Physical and environmental security: gives guidance on the protection of computer facilities;

(vii) Communications and operations: provides guidance on management of technical security controls in systems and networks;

48
(viii) **Access control:** provides guidelines for restrictions of access rights to networks, systems, applications, functions and data;

(ix) **Information systems acquisitions, development and maintenance:** provides instruction about building security into systems applications;

(x) **Information security incident management:** provides guidance on how to respond appropriately to information security breaches;

(xi) **Business continuity management:** gives guidelines on protecting, maintaining and recovering of business-critical processes and systems; and

(xii) **Compliance:** ensures conformance with information security policies, standards, guidelines, laws and regulations.

In this research work, the ISO-27002 twelve security control principles provided a good foundation for establishing the criteria for analysing and modelling eGMMs for security services. The modelling part was complemented by the socio-technical approach through the use of the SBC model [Kowalski, 1994]. Each of the evaluation criteria, technical and non-technical, were mapped to a number of security control elements from the ISO-27002 twelve security control principles, as described in Annex D–4, and summarised in research paper III. Additionally, the ISO-27002 twelve security control principles were used for developing parts of the framework, a catalogue of security service requirements control areas (SRCAs) for each of the eGMM stages. Annex E–3 shows how the ISO-27002 twelve security control principles were used to guide the development process of a catalogue of SRCAs. Results from table E–3, were then matched into table E–7, which has five critical maturity levels of ISMM, whereby each critical level has different types of SRCAs (security objectives, security processes and security metrics). All SRCAs were divided into technical and non-technical security services. Thereafter, table E–7 was transformed into tables E–8 and E–9. Tables E–8 and E–9 were intended for the SRCAs for the lowest and highest critical maturity levels of ISMM respectively. Annex C, and research papers V and VI shows in detail how the ISO-27002 twelve security control principles were applied to guide the studies, and also to develop part of a catalogue of SCRAs for the proposed framework.

### 3.4.2 ISO/IEC 21827: Systems Security Engineering Capability Maturity Model

The Systems security engineering capability maturity model (SSE-CMM) is considered to be the foundation for building maturity models such as information security maturity models whose security services maturity levels are designed in incremental order. The ordering is similar to that of e-government services in the eGMM stages. SSE-CMM is a security standard developed by the International systems security engineering association (ISSEA)\(^{54}\). Also, it is known as the ISO/IEC 21827 standard.

\(^{54}\) ISSEA is a non-profit membership organization focusing on the advancement of systems security engineering [SSE-CMM, 2003]
The main objectives of SSE-CMM were to address security engineering activities, in particular to secure system life cycles. The processes include products/system concepts definitions, requirements analysis, design, development, integration, installation, operations, maintenance and commissioning. Figure 3–10 below depicts the detailed snapshot of the five levels of SSE-CMM.

![Figure 3–10: SSE-CMM capability maturity levels [SSE-CMM, 2003, p.44]](image)

Level 1: performed informally, focuses on organizations when conducting processes that incorporate the base practices; level 2: planned and tracked, focuses on project definition, planning and performance issues; and level 3: well defined, focuses on defining the processes within an organization. Other levels are: level 4: quantitatively controlled, focuses on measurement being tied to the business goals of the organization, and level 5: continuously improving, deals with leveraging management practices improvement. In general the SSE-CMM is focused on security engineering and software design [SSE-CMM, 2003].

In this research work, SSE-CMM was applied for building the basis and foundation for analysing and developing enhanced ISMM levels. The modelling of ISMM maturity levels were guided by the SBC model security services requirements areas, technical and non-technical, as depicted in Annex E–2 and tables E–1 and E–2. Detailed analysis and development processes for the ISMM security maturity levels are outlined in research paper IV. Additionally, based on the established SRCAs, developed from the ISO-27002 twelve security control principles given in Annex E–3 table E–3, the SSE-CMM security services summarised in Annex E–3 table E–6 were matched into table E–3. Table E–3 was later transformed into table E–7, which has five critical maturity levels of ISMM. Thereafter, table E–7 was transformed into tables E–8 and E–9. Annex C, and research papers V and VI shows in detail how the SSE-CMM was applied to develop part of a catalogue of SCRAs for the proposed framework.
3.4.3 ISO/IEC 15408: The Common Criteria (CC)

The Common Criteria (CC) provides broad basis for achieving functional and assurance requirements for IT products, such as e-government systems applications and infrastructures. CC is an internationally approved set of security standards (ISO/IEC 15408) based on a framework that offers measurable levels of assurance for computer products and systems. CC certifications up to level 4 are mutually recognised among the members of the common criteria recognition arrangement (CCRA)\(^{55}\) which is an internationally recognised body. CC as a security standard has a long history as summarized in figure 3–11 below.

![Figure 3–11: CC development process [SANS, 2003b, p.1]](image)

The assurance process in CC, demands specifying, implementing and evaluating security features of the target of evaluation (TOE)\(^{56}\). The TOE security threats, objectives, requirements, and summary specification of security functions and the assurance measures together became the primary input to the security target (ST). The TOE encompasses the following security features [CC, 2009]:

(i) *Protection profile (PP)*: is the standard document that outlines procedures for defining independent set of security requirements and objectives for a category of products or systems which meet similar consumer needs for IT security. It comprises of security threats, policies, assumptions, objectives and rationale;

(ii) *Security target (ST)*: is the standard document that outlines procedures for identifying security properties of the target of evaluation. It contains the IT security objectives and requirements of a specific identified TOE. Also, it defines functional and assurance measures offered by the TOE to meeting the demanded requirements;

---

\(^{55}\) CCRA is an internationally recognised body responsible for ensuring that: products are evaluated by the competent and independent licensed evaluators for fulfillment of security properties; supporting documents are used within the CC certification process; and certification issued for the evaluated security properties of the products’ are recognized by all members of the CCRA [CC, 2009].

\(^{56}\) TOE refers to the product or system that is the subject of the evaluation process [CC, 2009]
(iii) **Security functional requirements (SFRs):** is the standard document that describes procedures for specifying and providing a standard catalogue for required security functionality. In addition, it establishes levels of confidence that may be placed in the products’ or systems’ security features through quality assurance processes;

(iv) **Security assurance requirements (SARs):** is the standard document that outlines procedures for describing security measures to be taken during development and evaluation of computer products and systems. It ensures compliance to the asserted security functionality; and

(v) **Evaluation assurance level (EAL):** is the standard document that outlines the description of the depth and rigor of an evaluation. Each EAL is aligned to a package of security assurance requirements (SARs). EAL-1 being the most basic, therefore cheapest to implement and evaluate, and EAL-7 being the most stringent and most expensive. However, EAL does not indicate the actual security capabilities of the product, but stipulates independently levels of evidence reviewed and functionally tested against the vendor’s claims.

In this research work, CC was used for providing and enhancing security services requirement control areas during the development of a catalogue of SRCAs for the proposed framework. Additionally, based on the established criteria for SRCAs, developed from the ISO-27002 twelve security control principles given in Annex E–3 table E–3 – CC security services summarised in Annex E–3 table E–5, were matched into table E–3. Table E–3 was later transformed into table E–7, and thereafter from table E–7 to tables E–8 and E–9. Annex C, and research papers V and VI show in detail how CC was applied to develop the SCRA catalogue for the framework for securing e-government services. Also, research paper VII shows how part of the framework’s catalogue of SRCAs were applied to develop a protection profile (PP) for a controlled electronic voting system while taking into consideration, technical and non-technical security issues in the target environment.

### 3.4.4 National Institute of Standard and Technology (NIST) on e-Government

The National institute of standard and technology (NIST)\(^\text{57}\) has maturity levels for security services which are designed in incremental order, which are similar to e-government services in eGMMs maturity stages. This gave a good basis for the model to be considered and applied in modelling security services in eGMMs.

NIST has developed a number of guiding documents for information security that could also be adopted and applied in enhancing e-government security services. These include: managing risk from information systems – an organisational perspective (NIST special publication 800-39), Risk management guide for information

\(^{57}\) Is a non-regulatory Federal Agency within the US department of Commerce founded in 1901, with its mission to “promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economy, security and improve quality of life” [NIST, 2008]
technology systems (NIST special publication 800-30), and the Methodology for evaluation information security maturity (ISM) of organisations (NIST IR7358). These documents present the framework for managing risks in an organisational environment. They further provide guidelines and directives on how to select, implement, and assess security controls. Additionally, they give instructions on how to monitor the states of security from an organisational perspective [NIST, 2008]. Moreover, NIST [2007b] identified five levels (aspects) that are necessary for any organisation to attain security maturity: an up-to-date security policy, security procedures, security implementation, security test, and security integration. According to NIST [2007b] higher level of maturity can only be attained if and only if the previous maturity level is attained. This implies that if there is no policy for a specific criterion, none of the maturity levels will be attained for the specific criterion. NIST is focused towards the level of security documentation.

In this research work, NIST was applied, along with other security maturity models, to develop the enhanced information security maturity model (ISMM), whereby five security maturity levels were developed. The modelling of ISMM levels was mostly guided by the SBC model security services requirements areas, technical and non-technical, as depicted in Annex E–2, tables E–1 and E–2. A detailed analysis and development processes for the ISMM security maturity levels are outlined in research paper IV.

3.4.5 Information Security Management Maturity Model (ISM3)

As for the previous security maturity models, Information security management maturity model (ISM3) has maturity levels for security services which are designed in incremental order, which are similar to e-government services in maturity stages of eGMMs. This gave good basis for the model to be applied in modelling security services in eGMMs.

ISM3 [2007] was proposed by the consortium for assessment and management of risk based processes oriented within organisations. The model has five security maturity levels: undefined, defined, managed, controlled, and optimized. The model offers a practical and efficient approach to managers and auditors for evaluating, specifying, implementing and enhancing process-oriented information security management systems. The strength of the model is based on the inclusion of coverage and capability maturity levels. ISM3 can be applied to any organization regardless of its size, context and resources. It gives a clear description of responsibilities for technical/operational personnel responsible for executing defined goals by means of technical processes. Tactical personnel deals with design and implementation of information security management systems; and strategic personnel deals with broad goals, coordination, and provision of resources. However, the current ISM3 (version 2.10) does not measure risk or security directly, nor does it provide best practices for security implementation. Metrics are process-based, measuring activities, scope, effectiveness, efficiency and quality. Every process in ISM3 is assumed to contribute
to the goal of information security management [ISM3, 2007]. Other information security maturity models are not shown here, but they were extensively analysed and presented in research paper IV [Karokola et al, 2011a].

In this research work, ISM3 was applied, along with other security maturity models, to develop the enhanced information security maturity model (ISMM), whereby five security maturity levels were developed. The modelling of ISMM levels was heavily guided by the SBC model security services requirements areas, technical and non-technical, as depicted in Annex E–2, tables E–1 and E–2. Detailed analysis and development processes for the ISMM security maturity levels are outlined in research paper IV. Furthermore, based on the established criteria for SRCAs, developed from the ISO-27002 twelve security control principles given in Annex E–3 table E–3, the ISM3 security services (summarised in Annex E–3 table E–4) were matched into table E–3. Table E–3 was later transformed into table E–7, and thereafter from table E–7 to tables E–8 and E–9. Annex C, and research papers V and VI show in detail how ISM3 was applied to develop a catalogue of SCRAs for the framework for securing e-government services.

3.5 Chapter Summary

This chapter outlined the description and understanding on the theoretical foundation and the underlying principles for modelling e-government services. The discussions looked into e-government maturity models and problem area, IT security terminologies in relation to e-government services, understanding of systems-thinking concepts, and how to identify, investigate, and model IT security problems. Lastly, descriptions of the mitigation measures for the identified IT security problem in eGMMs, and how they were applied was presented. The research results of the studies were reported in research papers published in peer-reviewed internationally recognised conferences and journals in information security and e-government. Also, they are summarised in chapter 4. Research papers’ extended summaries are outlined in chapter 5 and full papers are given in Part II of this thesis.

Table 3–2 below is an extended version of table 2–6 given in chapter 2. In the table, the applied holistic approaches and IT security mitigation measures are added. The table gives detailed summary on how each of the research studies were handle, from formulating the research questions, applied research methods and strategies, applied security holistic approaches and mitigation measures, to published research results in the form of research papers.
Table 3–2: Matrix for research studies, applied methods, strategies, and holistic approaches

<table>
<thead>
<tr>
<th>DSR Steps</th>
<th>Description</th>
<th>Awareness of the real-world problem</th>
<th>Suggestions for tentative design</th>
<th>Developing the framework</th>
<th>Evaluating the framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research study</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Research questions</td>
<td>I(a)</td>
<td>1</td>
<td>2(b)</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Research papers</td>
<td>I II III IV V VI VII</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applied methods &amp; strategies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QRM</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>QtRM</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case study</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survey study</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action research</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applied holistic &amp; other security approaches</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GST</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>SSM</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SBC</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO-27k</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSE-SMM</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISM3</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FraSeGoS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key:

Others – technology adoption models [Vankatesh et al, 2008]

FraSeGoS – A framework for securing e-government services [Karokola et al, 2012b],

The next chapter presents the research result, a framework for securing e-government services.
4. Results – A Framework for Securing e-Government Services

The chapter presents the research result, a framework for securing e-government services which integrates IT security services into e-government maturity models. The framework is presented in figure 4–1 below.
The framework presented in figure 4–1 was developed in response to the security problem in e-government services that is caused by many reasons including the lack of security services in eGMMs. eGMMs were purposely designed for guiding and benchmarking e-government implementation and service delivery in a stage-wise approach [Karokola et al, 2012a]. Security is a quality issue driven by a set of objectives [ISM3, 2007]. It should be included from the start and not at the later phases, such as during the planning, development, implementation, service delivery, and maintenance phases [Bishop, 2006; McGraw, 2005; Martins et al, 2002].

The proposed framework addresses both the quantity of offered e-government services and the quality of security services by aligning strategic objectives between e-government services and security services [Karokola et al, 2011a, 2011b, 2012a, 2012b]. It is expected that when the framework is appropriately implemented – it will mitigates the current and emerging security risks and threats posed to e-government services; hence enhances confidentiality, integrity and availability of critical information assets being stored, processed, and transmitted within and between e-government domains (G, B, and C) [Karokola et al, 2011a, 2011b, 2012a, 2012b]. All major research results were reported in the research papers, published in the peer-reviewed internationally recognised conferences and journals in information security and e-government. Extended summaries of the research papers are given in chapter 5, and full papers are included in Part II of this thesis.

The rest of the chapter is organised as follows: the chapter begins by describing the summary on how the entire research was conducted in order to address the identified security services gap in e-government services. This is followed by a brief description on how the proposed framework was evaluated. Finally, a description on how the proposed framework can be implemented to the government organisations is given.

4.1 How the Framework was Developed

The framework development processes were mainly guided by a design science research (DSR), shown in chapter 2.2 figure 2–2, complemented in parts by soft-systems methodology, systemic-holistic and socio-technical approaches. The applied DSR main steps were: awareness of the real-world problem, suggestions for tentative design, developing the framework (artifact), evaluating the proposed framework, and concluding the research results. To explicitly describe how the framework was developed – the development process is divided into five major steps and seven sub-steps as follows [Karokola et al, 2009a, 2011a, 2011b, 2012a, 2012b, 2012c]:
Step–1: Awareness of the real-world problem. An extensive literature review and case-studies were conducted in six government organizations located in Tanzania. The findings revealed that securing e-government services appears to be a major challenge; because security measures are implemented in an ad-hoc manner. Additionally, it was learned that implementation of e-government services in the targeted environment are heavily guided and benchmarked by eGMM, which is proposed by the Tanzanian national e-government strategy (TNGS) [Tz-eGov, 2008]. As underlined earlier, the TNGS recognizes the importance and use of eGMMs. It suggests the use of eGMM with four maturity stages which are similar to Gartner's model [Karokola et al, 2009a, 2012a; Tz-eGov, 2008]. However, the model lacks built-in security services, technical and non-technical [Karokola et al, 2012a]. Further, it was learnt that, some of the respondents were of the opinion that if the said model could have built-in security services, perhaps, it could have improved the security situation by enhancing alignment of the strategic objectives between e-government services and security services. This triggers for the need of investigating more eGMMs for security services [Karokola et al, 2009a, 2012a]. Therefore, based on the set criteria – eleven eGMMs were selected and extensively analysed for security services (for details, see sub-step–3.1 and research paper III). The findings revealed that they all lack security services in their maturity stages, technical and non-technical [Karokola et al, 2012a]. To create awareness of the identified security problems, these findings were communicated to the targeted organizations. Also, the findings were reported in research papers published in peer-reviewed internationally recognized conferences and journals in information security and e-government as research papers I, II and III.

Step–2: Suggestions for tentative design. In the previous studies, one of the identified security issues in the real-world environment that affect secure e-government services was the lack of security services, technical and non-technical, in eGMMs [Karokola et al, 2012a]. Addressing the identified security problem in eGMMs – it was important to propose a tentative design that would appropriately incorporate IT security services (both technical and non-technical) into eGMMs stages; hence securing e-government services. Consequently, several information security maturity models, standards and best practices were reviewed as presented in chapter 3 and research paper IV. Whereby information security maturity models (ISMMs) were identified as one of the possible measures for the identified security problem in eGMMs. The ISMMs were chosen because their security services are designed in a continuous incremental order from the lower to higher critical maturity levels; so as e-government services in eGMMs stages. Therefore, based on the set criteria, described in sub-step–3.2 and research paper IV, the selected ISMMs were extensively analysed for security services enhancement, technical as well as non-technical. The research results proposed five critical maturity levels of ISMM. In addition, based on other existing security standards and best practices, necessary security enhancements to the identified ISMM critical levels were made. The results are presented in detail in sub-step–3.2. Also, the results were reported in research paper IV.
Step–3: Developing the framework (artifact). The process involved utilizing suitable research approaches, methods and theoretical foundation from the existing theories in information security and e-government paradigm narrated in chapters 2 and 3. These includes General systems theory [Schoderbek et al, 1985], soft systems methodology [Checkland et al, 1990], systemic-holistic approach [Yngström, 1996], socio-technical modelling [Kowalski, 1994], and other information security maturity models, standards and best practices. Therefore, to explicitly describe how the framework development process (step) was achieved, it is divided into seven sub-steps as follows:

Sub-step–3.1: Identify maturity stages of eGMM. The internationally recognised e-government maturity models (eGMMs) were identified and extensively analysed for security services, as outlined in research paper III. The criteria for selection are given in the same research paper. The following eleven models were selected and analysed: Howard’s model [2001], WorldBank’s model [2003], Chandler & Emmanuel’s model [2002], Gartner’s model [Baum et al, 2000], and Layne & Lee’s model [2001]. Other models were: West’s model [2004], Hiller & Blanger’s model [2001], Moon’s model [2002], UN & DPEPA’s model [2008], Asia Pacific’s model [Wescott, 2004], and Deloitte & Touche’s model [2001].

The findings revealed the following: (i) security services, technical and non-technical, are lacking in eGMMs stages as summarized in table 14 of research paper III. (ii) the models were found to have different orientations in terms of the design and structures in relation to their maturity stages. Therefore, to address these requirements the following were undertaken: (a) addressing the security problem in eGMMs stages cited in item (i) above. Information security maturity models (ISMMs) were identified as the possible measures. This is presented in research paper IV and summarized in sub-step–3.2; (b) addressing the issue cited in item (ii), the selected eGMMs were analysed and synthesized [Walsh et al, 2005]. The results are summarized in table 15 of research paper III, whereby five maturity stages of a common frame of reference for eGMMs were proposed: web-presence, interactional, transactional, transformational, and continuous improvement. The maturity stages are described below. Also, they are presented in figure 4–2 on the vertical axis (Y) as eGMM stages [Karokola et al, 2012a]:

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 with provision of basic features and limited capabilities 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 and capabilities. 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. These results were reported in research paper III.

Sub-step–3.2: Identify critical maturity levels of ISMM. As outlined in Step–2, research paper IV, and chapter 3, an extensive literature review of different information security models, standards and best practices was conducted. Nevertheless, based on the nature of e-government services in eGMMs stages, they are designed in a continuous incremental order from the lower to higher maturity stages. Thus ISMMs were chosen because their security services are also designed in similar order. Consequently, based on the set criteria described in research paper IV, ISMMs were identified as the possible measure for addressing the current security problem in eGMMs cited in step–1 and in research paper III. In the process, eight internationally recognised ISMMs were selected. The models were: Information security management maturity model (ISM3) [ISM3, 2007], NIST (PRISMA) information security maturity model [NIST, 2007a], Generic security maturity model (GSMM) [Lessing, 2008; Neubauer, 2005], Gartner’s information security maturity model (GISMM) [Dzazali et al, 2009], and SUNY’s information security maturity model [Lessing, 2008]. Other models were: IBM–ISF information security framework [IBM-ISF, 2007], Citigroup’s information security maturity model [CitiGroup, 2000] and ISMS (Im) – maturity model [Woodhouse, 2008a].

The models were then analysed for security services enhancement, both technical and non-technical. Thereafter models with orientations to security awareness, evaluation, and management were synthesized [Walsh et al, 2005] for security services enhancement, whereby five critical security maturity levels with their respective security services were identified and proposed by the author. Furthermore, to affirm the findings a survey study was conducted in the targeted environment, six government organizations studied earlier. The results confirmed the proposition. The five ISMM critical security maturity levels were: undefined, defined, managed, controlled, and optimized. The critical maturity levels are described below. Also, they are presented in figure 4–2 on the horizontal axis (X) as ISMM critical levels [Karokola et al, 2011a, 2011b]:

Undefined maturity level: this is the lowest maturity level of information security model meant for organizations with low information security targets (IST)\(^58\) 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.

\(^58\) IST refers to security services requirements for a given information systems or IT product in question [CC, 2009].
**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. Furthermore, 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 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. Highest security risk reduction from technical and non-technical security threats occur. 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. These results were reported in research paper IV.

**Sub-step–3.3: Integrate critical maturity levels of ISMM into maturity stages of eGMM.** The maturity stages of eGMM (identified in sub-step–3.1) were arranged on the Y axis and the critical maturity levels of ISMM (identified in sub-step–3.2) on the X axis as shown in figure 4–2 below. Each critical maturity level of ISMM was mapped against the maturity stages of eGMM. The plotted values are on an ordinal scale level (rank order only) for both axes [Karokola et al, 2011b].

*Figure 4–2: Integrating ISMM critical levels into eGMM stages*
The figure allows two interpretations: (i) each of the maturity stages can ideally reach the highest security maturity level “optimised”. This is presented as capital letters (E, J, O, T and Y) in the progression between one maturity stage to another. (ii) in totality for eGMM stages to reach the highest level of security maturity – security requirements for each of the maturity stages may need to be developed progressively from “Undefined” to “Optimized”. These maturity levels were named as maturity sub-levels of ISMM. Maturity sub-levels of ISMM are created to be within each of the security critical maturity levels of ISMM. This is presented in figure 4–2 as capital letters (A–E, F–J, K–O, P–T, and U–Y) on the continuum within e-government maturity stages and security maturity levels. The identified ISMM sub-levels are described as follows [Karokola et al, 2011b]:

**Undefined maturity sub-level:** this is the lowest maturity sub-level of information security meant for e-government services operated 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 sub-level:** is the second maturity sub-level meant for e-government services operated in a normal security risk environment. At this level, security policies including awareness, visions, and strategies are reviewed and updated. In addition, security risk reduction from technical and non-technical security threats occurs.

**Managed maturity sub-level:** this is the advanced level than sub-level two meant for e-government services operated 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 sub-level:** is the fourth maturity sub-level of information security meant for e-government services operated in a normal or higher security risk environment; highest security risk reduction from technical and non-technical security threats occurs. Security policies, awareness, visions, and strategies are regularly reviewed and updated.

**Optimized maturity sub-level:** this is assumed to be the highest maturity sub-level. It is meant for e-government services operated in higher security risk environment. Highest security risk reduction from technical and non-technical security threats occurs. Security policies, awareness, visions, and strategies are regularly reviewed and updated.

**Sub-step–3.4: Integrate different types of security services requirements control areas.** To integrate different types of security services requirements control areas (SRCAs) – figure 4–2 is transformed into a tabular form as shown in table 4–1 below. The table introduces one aspect of maturity stages in relation to security services in maturity levels of ISMM. All levels of ISMM are divided into technical “referred to as tech” and non-technical “referred to as non-t” security services requirements. Technical security aspects include hardware and software solutions such as access control and antivirus mechanisms; whilst non-technical security aspects

---

59 ISMM sub-levels for U, V, W, X and Y, i.e (U – Y) are not shown on the plotted graph, figure 4–2, but they are shown in table 4–1.

60 Security maturity sub-levels (undefined, defined, managed, controlled, and optimized) are designed to be within each of the critical maturity levels of ISMMs. Implementation of the security services from the security maturity sub-levels may not necessarily be followed sequentially, but organizations has to make sure that security requirements for that particular critical maturity level of ISMM are appropriately met.
include ethical and cultural norms, legal and contractual documents, administrative and managerial policies, operational and procedural guidelines, and awareness programmes [Karokola et al, 2009a, 2011a, 2011b, 2012a].

Additionally, to effectively identify security services requirements for each maturity stage of eGMM – the maturity sub-levels of ISMM, presented in capital letters “A – Y” in figure 4–2, were integrated into maturity stages. Table 4–1 shows the integrated maturity sub-levels of ISMM into the maturity stages of eGMM. Additionally, to comprehensively integrate security services requirements into the maturity stages of eGMM – it was important to identified types of security services requirements control areas (SRCAs) required at each of the maturity sub-levels. The identified types of SRCAs were: Security objectives\(^{61}\), security processes\(^{62}\), and security metrics\(^{63}\) assessment [CC, 2009; ISM3, 2007; ISO-27K, 2005; Karokola et al, 2011b; Owasp, 2009; SSE-CMM, 2003]. Further, the proposed SRCAs were divided into technical and non-technical security services. In the table, these SRCA were titled as objective, processes and metrics [Karokola et al, 2011b].

Table 4–1: Matrix for integrating SRCA into ISMM critical levels and eGMM stages

<table>
<thead>
<tr>
<th>ISMM Levels</th>
<th>Defined</th>
<th>Managed</th>
<th>Controlled</th>
<th>Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturity Stages</td>
<td>Undefined</td>
<td>Defined</td>
<td>Managed</td>
<td>Controlled</td>
</tr>
<tr>
<td>eGMM</td>
<td>Tech</td>
<td>Non-T</td>
<td>Tech</td>
<td>Non-T</td>
</tr>
<tr>
<td>Continuous improvement</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
</tr>
<tr>
<td>Transformation</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
</tr>
<tr>
<td>Transaction</td>
<td>K</td>
<td>L</td>
<td>M</td>
<td>N</td>
</tr>
<tr>
<td>Interaction</td>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
</tr>
<tr>
<td>Web-presence</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
</tbody>
</table>

\(^{61}\) Security objectives refer to intent to achieve confidentiality, integrity and availability of services;

\(^{62}\) Security processes refer to activities that defines information security implementation practices and procedures;

\(^{63}\) Security metrics refer to indicators which provide qualitative and quantitative measures of security maturity and assurance; metrics are critical as they often used to predict future behaviour and trend of a system.
Sub-step–3.5: Transform the table into pictorial presentation. To clearly show the integration of the identified types of SRCAs into eGMM stages and ISMM critical maturity levels and sub-levels, the above table 4–1 is transformed into a pictorial presentation shown in figure 4–3. In the figure, the first column (FIS–1) shows the main goal of the framework “a secured eGMM”, whereas FIS stands for framework implementation step. The second column (FIS–2) refers to the available options for e-government services in eGMM stages: web-presence, interaction, transaction, transformation, and continuous improvement. The third column (FIS–3) gives possibilities for the available options for security services, technical and/or non-technical. And the fourth column (FIS–4) refers to the available different types of security services requirements control areas (SRCAs): security objectives, security processes, and security metrics. These are linked to the technical and non-technical security services. The last column (FIS–5) refers to the available options for SRCAs in ISMM critical levels: undefined, defined, managed, controlled and optimized.

Furthermore, as discussed above, ideally each critical maturity level of ISMM has maturity sub-levels: undefined, defined, managed, controlled and optimized, marked in capital letters as A – E, F – J, K – O, P – T, and U – Y respectively. The maturity sub-levels were then integrated into their respective critical maturity levels as shown in FIS–5. Thereafter, the security services selection matrix between FIS–4 and FIS–5 was introduced. Lastly, the framework implementation steps (FISs) were grouped into framework implementation phases (FIPs). FIP–1 being for e-government services related activities, comprising of FIS–1 and FIS–2; whilst FIP–2 being for security services related activities, comprising of FIS–3, FIS–4 and FIS–5 [Karokola et al, 2011b].

Sub-step–3.6: Introduce the feed-back security control system mechanisms. In table 4–1 and figure 4–3, the security services requirements i.e., for Web-presence maturity stage, could ideally be in progression from undefined, defined, managed, controlled to optimised sub-levels of ISMM referred to (in capital letters) as A, B, C, D and E, respectively. This suggests that the security services requirements from the lower sub-levels may become an input to the higher ones. Therefore, the security problem in e-government is treated as an open system that interacts with its environment, the operating environment. According to the general system theory, an open system is a system whose boundaries permits flow of information in and out of the system. It consists of input (I), process (P), output (O), and feed-back [Schoderbek et al, 1985]. When translating this into figure 4–3 under FIS–5, it suggests that output from the lower maturity sub-level of ISMM, after being processed, becomes input to higher maturity sub-levels. The same mechanism is applied to critical maturity levels of ISMM. Therefore, the feedback security system mechanisms with input (I), process (P), output (O), and feed-back is introduced between the ISMM levels and sub-levels, repetitively, from the lower to the higher levels and sub-levels, as depicted in figure 4–3 below [Karokola et al, 2011b].
Figure 4–3: A framework for securing e-government services which integrates IT security services into eGMMs (version 1)
Sub-step–3.7: Develop a catalogue of security services requirements control areas. A comprehensive catalogue of security services requirements control areas (SRCAs) for the identified maturity levels/sub-levels was developed, for detail see Annex C. The SRCAs development process was based on the existing standards, models and best practices such as ISO-27000 family [2005], Systems security engineering capability maturity model [2003], Common criteria [2009], and Information security management maturity models [2007]. The ISMM critical levels security services requirements control areas (SRCAs) development, matching, and testing processes involved a group of Master and PhD students in the area of information and communication systems security (ICSS) from the department of computer and systems sciences, Stockholm University/Royal Institute of Technology, in Sweden. Further details are given in chapter 2.5.3 and research paper V. Annex C shows the developed catalogue of SRCAs. In Annex C – I, the first column present names for ISMM levels/sub-level referred to as FIS–5. The second column presents types of the security services requirements control areas denoted as technical and non-technical referred to as FIS–3. The third and fourth columns depict different types of SRCAs: security objectives, security processes, and security metrics and their descriptions referred to as FIS–4. The last three columns outline the mapped SRCAs referenced from Annexes C – II, III, IV and V. they are referred to as FIS–5.

It is worth mentioning that depending on the criticality of e-government services (to be implemented and secured) organisations may not necessarily follow the sequential ordering of the security maturity sub-levels within the critical maturity levels 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/s of ISMM are appropriately met. One of the possible ways for measuring the levels of security services maturity, if they have been met, could be by either conducting an evaluation based on security threats profile, security risks profile or business impacts, by balancing the impact of security threats with appropriate security measures (safeguards). It is important for organizations to cost-effectively mitigate associated security risks and threats posed to e-government services. Else, re-defining of the strategic objectives between e-government services and security services is necessary. These results were also reported in research paper V [Karokola et al, 2011b].

Step–4: Evaluating the proposed framework (performance measures). This is the most important step of this research work. It provides essential feed-back to the framework development processes and quality assurance. The design process is iteratively performed from the awareness of the real-world problem, suggestions of a tentative design, developing a framework to evaluating the proposed framework, until the real-world situation is improved. Based on the analysis of the evaluation methods, presented in chapters 2.5.4 and 4.2 and in detail in research paper VI, a theoretical evaluation method was chosen, whereby a case-study was adopted as an evaluation tool of the proposed framework. The framework evaluation results indicated that it was widely accepted by the targeted organizations in Tanzania. Respondents from the organisations at different levels (strategic, tactical, and operational) had expectations
that the framework would assist them in mitigating the current and emerging security risks and threats posed to e-government services. The improved version of the framework is shown in figure 4–1/4–7 along with a catalogue of SRCAs given in Annex C. However, the author acknowledges the framework limitations given in chapter 6.4. A detailed description of the framework evaluation process is given in the next section, chapter 4.2. Also, the findings were reported in research paper VI [Karokola et al, 2012b].

**Step–5: Concluding the research results.** The final research result was a framework for securing e-government services which integrates IT security services into eGMMs stages. All research results that contributed to the development process of the framework were reported in seven research papers, marked as paper I to VII. The research papers were published in the peer-reviewed internationally recognised conferences and journals in information security and e-government. Extended summaries of the papers are given in chapter 5. Also, full papers are presented in Part II of this thesis. Additionally, chapter 6 includes concluding remarks of this research work.

4.2 **How the Framework was Evaluated**

Evaluation is one of the most important steps in framework (artifact) development. It provides essential feedback to the framework development and the quality assurance process. The design process is iteratively performed from the awareness of the real-world problem, suggestions of a tentative design, developing a framework to evaluating the proposed framework until the real-world situation is improved (for details see chapter 2.2, figure 2–2). There are a number of evaluation methods that could be used for evaluating the proposed framework. They include observational, descriptive, analytical, testing and experimental methods [Guba, 1981; Hevner et al, 2004; Zelkowitz et al, 1998]. These methods were extensively analysed and presented in chapter 2.5.4, and in research paper VI, whereby observational and descriptive evaluation methods appeared to be more suitable for a theoretical evaluation approach. Similarly, analytical, testing and experimental methods appeared to be more suitable for a practical evaluation approach. The practical evaluation approach requires implementing the framework in the real-world environment (organisations), by applying the framework in an e-government project. The process would demand much time, as well as resources.

Therefore, because lack of time was the major obstacle when evaluating the proposed framework, a theoretical evaluation approach was chosen. A case-study was selected for conducting the study in the same organisations studied earlier [Karokola et al, 2011a; Yin, 1994]. Further, questionnaires for guiding the evaluation process of the proposed framework was developed [Davis, 1989; Guba, 1981; Hevner et al, 2004; Venkatesh et al, 2008; Zelkowitz et al, 1998]. The questionnaire had seven evaluation criteria: simplicity, coverage and completeness, compliance to security standards, and dynamics and flexibility. Other criteria were: capability and relevance, usefulness, and
trustworthiness, for detail see Annex F of this thesis. It is important to note that since the purpose of the framework evaluation was to get feed-back for improvements, research results of the ratings for those who agreed and strongly agreed are presented here. Ratings for those who were either not sure, disagreed or strongly disagreed are not shown here [Karokola et al, 2012b]:

What follows is a summary description of the framework evaluation results. The results from the data processing and analyses were divided into three major parts: the first part (Part–1) analyses overall acceptability ratings of the proposed framework regarding the seven evaluation criteria; the second part (Part–2) gives a comparative analysis of the acceptability ratings among the groups levels within the organisations (strategic, tactical and operational); and the third part (Part–3) addresses areas of framework improvements, which is based on the respondents' opinions. The total number of respondents is given in chapter 2.5.4 table 2–5 [Karokola et al, 2012b]:

Part–1: Analysis of the acceptability ratings for the proposed framework. The research results for the evaluation of the proposed framework in this category are grouped into the following: overall acceptability ratings, and acceptability ratings according to organisation (U – Z):

Overall acceptability ratings of the proposed framework: based on the established seven evaluation criteria, the compiled results from the surveyed organisations are discussed below. Further, figure 4–4 below presents the summary of the research results:

  Simplicity criterion: the overall acceptability rating was at 78% as depicted in figure 4–4 below. 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 in the overall acceptability rating of the framework for this criterion compared to the former one. The rating was at 88% as depicted in figure 4–4. This suggests that respondents perceived the framework to adequately address technical, non-technical, practical, and theory-related security issues.

  Compliance to security standards criterion: the overall acceptability rating was at 92% as shown in figure 4–4. 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 of the acceptability rating to 76% compared to the former criterion as depicted in figure 4–4. This suggests that respondents perceived the framework to be dynamic and flexible enough to deal with

64 It should be noted that the number of respondents at the strategic level is small compared to those at the tactical and operational level. The strategic level had 7 respondents, the tactical level had 32 respondents, and the operational level had 30 respondents. From this follows a change of opinion of any personnel at the strategic level will result in a change on the acceptability ratings of app. 14%; whilst change of opinion of any of the respondents at the tactical level or the operational level will be app. 3%.
possible future security risks and threats facing e-government implementation and service delivery.

Capabilities and relevance criterion: there was an increase for acceptability rating for this criterion to 77% compared to the former one as depicted in figure 4–4. This suggests that respondents perceived the framework to be feasible when dealing with security risks and threats facing e-government services.

Figure 4–4: Overall acceptability ratings of the framework using seven different evaluation criteria for all organizations (U–Z)

Usefulness criterion: there was an increase for the acceptability rating to 95% compared to the former criterion as depicted in figure 4–4. 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 4–4. Generally, respondents perceived that it is fairly worth trusting the framework for mitigating security risks and threats facing e-government services.

Acceptability ratings of the proposed framework according to organisation (U–Z): based on the established evaluation criteria, the research results from the six surveyed organisations are discussed below. Further, figure 4–5 below presents the summary of the research results:

Simplicity criterion: acceptability ratings for the proposed framework among the six organisations showed that organization W rated the framework highest at 99%, followed by organization U at 92%. Organization Y rated it lowest at 55%. This
suggests that the framework design was rated as more easily understandable to personnel in organisation W than those in organisation Y. These differences among organisations could depend on many reasons, including types of e-government services offered by the organisations, and also on the personnel technical skills and expertise regarding security related issues. Figure 4–5 shows the summarised results.

Coverage & completeness criterion: acceptability ratings for the proposed framework among the six organisations showed that Organization X rated the framework highest at 99%, followed by organization Y at 91%. Organization Z rated it lowest at 80%. The results suggest that respondents at organisation X perceived the framework to adequately address technical, non-technical, practical, and theory-related security issues than those at organisation Z. Figure 4–5 below shows the summarised results.

Compliance to security standards criterion: acceptability ratings among the six organisations showed that organizations V, W and X 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 to the current security standards and best practices. Figure 4–5 shows the summarized results.

Dynamics and flexibility criterion: acceptability ratings among the six organisations showed that organization U rated it the highest at around 99%, whilst organisation X rated it the lowest at 63%. This suggests that respondents in organisation U they perceived the framework to be dynamic and flexible enough to deal with possible future security risks and threats facing e-government
implementation and service delivery than those in organisation X. Figure 4–5 show the
ratings.

Capabilities and relevance criterion: acceptability ratings among the six
organisations showed that organization U rated the framework highest at 92%, whilst
organisation Y rated it the lowest at 64%. This suggests that respondents in
organisation U perceived the framework to be more feasible when dealing with
security risks and threats posed to e-government services than those in organisation Y.
Figure 4–5 shows the ratings.

Usefulness criterion: acceptability ratings among the six organisations showed
that organization U, W and X rated the usefulness of the framework highest at around
100%, while organization V rated it lowest at 85%. These results suggests that
respondents in organisations U, W and X perceived the framework to be more useful
when dealing with mitigating security risks and threats posed to e-government services
than those in organisation V. Figure 4–5 shows the ratings.

Trustworthiness criterion: acceptability ratings for the six organisations showed
that organization W rated the framework highest at 90%, whilst organization V rated it
the lowest at 62%. These results suggest that respondents in the organisations W
perceived the framework to be more trustworth for mitigating security risks and
threats facing e-government services than those of organisation V. Figure 4–5 shows
the detailed ratings.

Part–2: Comparative analysis of the framework acceptability ratings between the
three group levels (strategic, tactical and operational). The research results for the
comparative analysis of the acceptability ratings of the proposed framework among six
surveyed organisations are presented below and summarized in figure 4–6:

Simplicity criterion: comparative analysis shows that there was fairly low variation
of about 1% between the strategic and tactical level. Further, there was slightly higher
variation of 14% between the tactical and operational level. This suggests that
respondents at the strategic and tactical level had more or less the same ratings on the
framework simplicity compared to those between strategic and operational levels.
Figure 4–6 depicts the variation of acceptability ratings in detail.

Coverage and completeness criterion: there was fairly low variation of about 9%
between strategic and tactical level. Also, variation between tactical and operational
level was at 11%. The implication here is that directors were more confident with the
framework security services coverage and completeness than managers and
operational personnel. The variation of acceptability ratings are depicted in figure 4–6.

Compliance to security standards criterion: there were fairly small variations
among the group levels on the framework acceptability ratings. The variation between
strategic and tactical level was at 9%. Additionally, there was very low variation of
about 0.6% between the tactical and operational level. This suggests that respondents
at the tactical and operational level had similar ratings on the framework compliance
to security standards and best practices. The variation of acceptability ratings are depicted in figure 4–6.

**Dynamics and flexibility criterion:** comparative analysis shows that there were higher variations between the groups on the framework acceptability ratings. Variation between the strategic and tactical level was at 38%. And between the operational and the tactical level was 24%. This implies that personnel at the strategic level were more confident than those at tactical and operational levels; also, personnel at the operational level were more confident than those at the tactical level. The variation of acceptability ratings are depicted in figure 4–6.

![Figure 4–6: Comparative analysis of framework acceptability ratings using evaluation criteria, among organizational levels: strategic, tactical and operational](image)

**Capabilities and relevance criterion:** comparative analysis shows that there was higher variation in acceptability ratings for the framework among the organizational levels. Variation between 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 showed more confidence compared to those at the tactical and operational level. The variation of acceptability ratings are depicted in figure 4–6.

**Usefulness criterion:** comparative analysis shows that 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 level was at 0.4%. This suggests that personnel at the tactical and operational levels had more or less the same ratings on the framework usefulness when dealing with security risks and threats facing e-government services. The detailed variation of acceptability ratings are depicted in figure 4–6.
Trustworthiness criterion: comparative analysis shows that there was high variation in acceptability ratings for the framework among the group levels. The variation in trustworthiness acceptability ratings between the strategic and tactical level was at 19%. And that between tactical and operational level was at 11%. This suggests that personnel at strategic level trusted the framework more than those at tactical and operational levels. Figure 4–6 depicts the variation of acceptability ratings in detail.

Part–3: Analysis of areas of framework improvement. There were a number of comments/ opinion given by the respondents from the surveyed organisations aimed at improving the framework. They are summarized and analysed in table 4–2. In the table, the first column names the framework evaluation criteria. The second column narrates the respondents’ opinions with respect to areas of framework improvements. The last column summarizes measures taken to address the given opinions.

Table 4–2: Summary of a framework’s areas of improvements

<table>
<thead>
<tr>
<th>Framework Evaluation Criteria</th>
<th>Proposed Areas of Framework improvements</th>
<th>Improvement made to the Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplicity</td>
<td>The framework is clear and easily understandable to intended users</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>
</tr>
<tr>
<td>Coverage &amp; completeness</td>
<td>The framework adequately addresses: technical, non-technical, practice, and theory related security issues</td>
<td>To include SRCAs for the other ISMM sub-levels: undefined, defined, managed, and controlled</td>
</tr>
<tr>
<td>Compliance to security standards</td>
<td>The framework is aligned with current 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>
</tr>
<tr>
<td>Framework Evaluation Criteria</td>
<td>Proposed Areas of Framework improvements</td>
<td>Improvement made to the Framework</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Dynamics &amp; flexibility</td>
<td>The framework is dynamic enough to deal with possible future 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>

**Note:** No comments/opinion was received regarding the following criteria: capability and relevance, usefulness, and trustworthiness.

Given the nature of opinions collected from the respondents the framework areas of improvements were categorized into graphical and descriptive presentations. Graphically, the framework visualization was improved from the earlier version presented in figure 4–3 to the current one presented in figure 4–7. The improvements made include simplification and enhancement of the selection process for security services requirement control areas (SRCAs), whereby the number of interconnections (matrix) in the implementation phase FIP–2, i.e. between FIS–4 and FIS–5 has been reduced. Also, the ISMM sub-levels (A–E, F–J, K–O, P–T, and U–Y) given under FIS–5 were re-organised within the ISMM critical levels. Additionally, the word “security” was added at each of the three security services control areas given in FIS–4. Figure 4–7 shows the improved version of the framework.

Additionally, the catalogue of security services requirements control areas (SRCAs) given in Annex C was descriptively enhanced. Based on the given opinions, most of the SRCAs were revisited and improved including the ones from the Common criteria (CC) and Systems security engineering capability maturity model (SSE-CMM). Nevertheless, other opinions on the framework's areas of improvement were not implemented at this stage, due to several factors including time limitations. But they are noted for further research work, discussed in chapter 6.4. No opinions were given for improving the framework for the capability and relevance, usefulness, and trustworthiness criteria. The enhanced framework is given in figure 4–7 along with the catalogue of SRCAs given in Annex C.

Therefore, based on the analyses and discussion presented in Part–1 and Part–2, the results indicated that the proposed framework was widely accepted by the surveyed organizations. Respondents from the organisations at different organizational levels (strategic, tactical, and operational) have high expectations that the framework would assist them in mitigating current and emerging security risks and threats posed to e-government services. However, the author acknowledges the limitations of the proposed framework, discussed in this section and outlined in chapter 6.4. These results were also reported in research paper VI [Karokola et al, 2012b].
4.3 How the Framework can be Implemented

This section presents the description on how the proposed framework presented below can be implemented into the government organisations.

Figure 4–7: A framework for securing e-government services which integrates IT security services into eGMMs (version 2)
To simplify the framework implementation process, it is divided into two main phases, referred to as framework implementation phases (FIP). Phase one is intended for implementing e-government services marked as FIP–1, whilst phase two is all about implementing security services for the identified e-government services in FIP–1, marked as FIP–2.

What follows is the description for each of the above mentioned implementation phases along with their respective framework implementation steps (FIS) [Karokola et al, 2011b, 2012b]:

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

- 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 are 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); the maturity stages are: web-presence, interactional, transactional, transformational, and continuous improvement (they are defined in chapter 4.1 sub-step–3.1). At this implementation 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 of eGMM, identifying its functional requirements that will facilitate smooth implementation of the service, and thereafter its required implementation process. 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 1, FIP–1. The phase implementation is divided into three implementation steps marked as FIS–3, FIS–4 and FIS–5:

FIS–3: Identify types of security services to be implemented. Refers to types of demanded security services requirement control areas (SRCAs) given in a catalogue: technical and/or non-technical security aspects. 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 type of e-government services selected in FIS–2, e-government implementers will be able to appropriately identify security services requirement, either technical and/or non-technical.

FIS–4: Identify different types of security services requirements control areas. Refers to different types of demanded security services requirement control areas (SRCAs) related to technical and/or non-technical; namely: 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 C–1.

FIS–5: Identify different types of the required security maturity levels with their respective security services requirements control areas. Refers to different types of SRCAs available in the critical maturity levels of information security maturity model (ISMMs); the ISMM critical levels are: undefined, defined, managed, controlled, and optimized (maturity levels are defined in chapter 4.1 sub-step–3.2). It is important to note that ideally each of the five critical maturity levels has maturity sub-levels within it: undefined, defined, managed, controlled and optimised (sub-levels are defined in chapter 4.1 sub-step–3.3). They are marked 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. 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 to 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 (I), processes (P), and outputs (O).

Therefore, e-government implementers will be able to strategically identify appropriate ISMM critical level/s followed by the selection of the desired ISMM sub-levels security services requirements from the catalogue of SCRAs given in Annex C–1. 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 are 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 defined above.

Depending on the criticality 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, such as 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 the levels of security services maturity, if they have been met, could be by either conducting an evaluation based on security threats profile, security risks profile or business impacts by balancing the impact of security threats with appropriate security measures (safeguards).

It is important for organizations to cost-effectively mitigate associated security risks and threats posed to e-government services; else, re-defining of the strategic objectives between e-government services and security services to cost-effectively mitigating such security risks and threats is necessary.

Framework limitations: the author acknowledges that currently the proposed framework has some limitations mentioned in chapter 6.4. The limitations are considered for further research work.

4.4 Chapter Summary
The chapter presented description of the proposed framework, a framework for securing e-government services which integrates IT security services into e-government maturity models. The description on how the framework was developed, how the framework was evaluated, and how the framework can be implemented into government organizations was extensively presented. All major research results presented in this chapter were also reported in seven research papers published in peer-reviewed international recognised conferences and journals in information security and e-government. The next chapter presents extended summaries of the included peer-reviewed published research papers.
Chapter 5

5. Summary of the Included Publications

This chapter presents extended summaries of the included research papers published in the peer-reviewed professional and academic international conferences and journals in information security and e-government. Full versions of the research papers are given in Part II of this thesis.

5.1 Summary of Research Paper I


My contribution: I was the main author of the paper.

Problem addressed: this is one of the preliminary papers that extensively explore IT security issues and challenges (technical and non-technical) affecting secure e-government services in the developing regions, where Tanzania was selected.

Methodology used: the study utilized qualitative and case-study as a research method and strategy respectively. The strategy was employed for data collection instruments preparation and data collection. Processing and analyses of descriptive and analytical/simple statistical data employed the use of content analysis and Microsoft excel tool respectively. Additionally, a systemic–holistic approach adopted from Yngström [1996] was applied to extensively investigate and analyse security issues and challenges, technical and non-technical, affecting secure e-government services in the study environment, where six government organizations were investigated.

Major findings: research results revealed that there are a number of security issues and challenges, technical and non-technical, which affect secure e-government services (implementation and service delivery) in the studied environment. These include: security services are implemented in an ad-hoc manner; personnel in IT security were not adequately trained; existence of low level of security awareness among some IT personnel and users of e-government services; and lack of management support and budgetary and economical issues that affect the procurement of security services measures. Further, it was learned that e-government implementation and service delivery is heavily guided and benchmarked by e-government maturity models (eGMMs) that appeared to lack built-in security services within their maturity stages. Additionally, in the course of the study, some respondents suggested that one of the possible ways for achieving secure e-government services could be by ensuring that eGMMs have built-in security services within their maturity stages. In this way, e-government implementers would be able to, while planning for e-government implementation and service delivery, also be able to plan for security
services requirement implementation; hence, achieving alignment of strategic objectives between e-government services and security services.

A full research paper is made part of this thesis in Part II. Also, it is available in the proceedings of the 5th International Conference on e-Government (ICEG 2009), pp. 91 – 100. Boston, USA. October, 2009. ISBN: 978-1-906638-49-8.

5.2 Summary of Research Paper II


My contribution: I was the co-supervisor to the main author during her Master’s thesis. In this paper, I was the co-author of the paper. I participated in initiating the work, refining the data collection instrument (questionnaire) and supervised the undertaking. Additionally, I participated in interpreting the outcome of the data analysis and quality check. Furthermore, I participated in structuring and writing the paper, and also in improving the paper, based on the peer-reviewers comments.

Problem addressed: the paper presents a case-study for secure e-government services adoption in Tanzania, whereby possible ways that would facilitate secure adoption and usage of e-government services were investigated. Further, the study compares the adoption processes of e-services for both private and public organisations.

Methodology used: the study utilized a mixed research methods that combines the use of qualitative and quantitative data. Further, the study employed case-study as a research strategy. The strategy was applied for questionnaire preparation and data collection undertaking. Processing and analyses of descriptive and statistical data employed the use of content analysis and Microsoft excel tool respectively. The study also reviewed different adoption models, whereby seven hypotheses were constructed.

Major findings: the results show that out of seven constructed hypotheses, only four were supported. The supported hypotheses were: perceived usefulness had a positive influence on the behavioural intention and use of e-government services; perceived trust had a positive influence on the behavioural intention of users on the usage of e-government services; higher levels of perceived IT security had a positive and a significant effect on perceived trust; and behavioural intention had a direct and positive effect on the actual usage and adoption of technology of e-government services. Additionally, in the course of the research study it was learned that private organizations appeared to be early adopters of technology and offer more secure e-services sooner than public organizations.

A full research paper is made part of this thesis in Part II. Also, it can be downloaded from the proceedings of the European Security Conference (ESC 2011), pp. 18 – 32. Örebro, Sweden. June, 2011.
5.3 Summary of Research Paper III


My contribution: I was the main author of the journal paper.

Problem addressed: e-government offers many benefits to the government (B), citizens (C) and the business community (B). However, e-government services are prone to current and emerging security challenges (technical and non-technical) posing potential risks and threats to critical information assets. Securing information appears to be a major challenge facing governments globally. On the other hand, e-government implementations and service delivery are heavily guided and benchmarked by e-government maturity models (eGMMs) having different maturity stages. Preliminary findings show that the models lack built-in security services, technical and non-technical. Therefore, the paper outlines an extensive investigation and analysis of eleven internationally recognised eGMMs for security services.

Methodology used: the study utilizes qualitative as a research method and survey study as a research strategy. In addition, the Soft systems methodology (SSM) of scientific inquiry/learning cycle adopted from Checkland and Scholes [1990] was applied to guide the study. Further, to establish the evaluation criteria for security services requirements in eGMMs stages, the ISO-27002 twelve security control principles, and Security-By-Consensus models [Kowalski, 1994] were applied. Based on the set selection criteria, eleven internationally recognised eGMMs were selected and thoroughly analysed for security services, technical and non-technical.

Major findings: the following were the major research results: (i) security services, technical and non-technical, were lacking in the maturity stages of eGMMs. Implying that eGMMs were designed to rather measure quantity of offered e-government services than quality of security services. (ii) eGMMs were found to have different orientations in terms of their design and structures in relation to their maturity stages. Therefore, addressing these observed issues in eGMMs, as a step towards achieving secure e-government services (addressing issue ii), a common frame of reference for eGMMs with five maturity stages was proposed. The proposed maturity stages were: web-presence, interactional, transactional, transformational, and continuous improvements. As a further work (addressing issue i), the proposed maturity stages of a common frame of reference for eGMMs will be extended to include the required security services, technical and non-technical.

5.4 Summary of Research Paper IV


My contribution: I was the main author of the paper.

Problem addressed: the paper outlines the proposition for a comprehensive information security maturity model (ISMM) that addresses both technical and non-technical security aspects. The proposed model is intended for securing e-government services (implementation and service delivery) in an emerging and increasing security risks and threats environment.

Methodology used: the study applied qualitative as a research method and survey study as a research strategy. The strategy was applied for questionnaire preparation and data collection undertaking. Processing and analyses of descriptive and analytical/simple statistical data employed the use of content analysis and Microsoft excel tool respectively. Additionally, the study utilized a holistic approach. The study was structured to a large extent by the security controls adopted from the Security-By-Consensus (SBC) model [Kowalski 1994]. Based on the set criteria, eight internationally recognised ISMMs were selected and extensively analysed for security services enhancement, technical and non-technical. Further, based on the models’ strengths, models with orientation towards security awareness, evaluation and management were selected for further enhancement. Models were then synthesised, whereby five critical maturity levels were proposed. To affirm the findings, a survey study was conducted into six government organizations, targeted in the previous research studies, located in Tanzania.

Major findings: a comprehensive ISMM with five critical maturity levels was proposed: undefined, defined, managed, controlled and optimized, along with their respective security services requirements, technical and non-technical. The main contribution of the study is the proposed model that addresses comprehensively security services requirements, technical and non-technical, within the critical maturity levels. Additionally, these findings would enhance awareness and understanding on the needs for security in e-government services to stakeholders.

5.5  Summary of Research Paper V


My contribution: I was the main author of the paper.

Problem addressed: e-government services, implementation and service delivery, is heavily guided and benchmarked by e-government maturity models (eGMMs). However, the models lack security services, technical and non-technical, in their maturity stages. The paper proposes a comprehensive framework for securing e-government services, which integrates IT security services into eGMMs stages.

Methodology used: the research utilized a qualitative as a research method and action research as a research strategy. Additionally, the study was guided by holistic approaches such as the Soft systems methodology (SSM) of scientific inquiry adopted from Checkland and Scholes [1990]. In the process, security services requirements (technical and non-technical) from the information security maturity model (ISMM) critical levels [Karokola et al, 2011a] were integrated into e-government maturity model (eGMM) stages [Karokola et al, 2012a] for the purpose of developing a framework for securing e-government services.

Major findings: a framework for securing e-government services which integrates IT security services into eGMMs was proposed. Additionally, a more comprehensive catalogue of security services requirements control areas (SRCAs) for securing e-government services was proposed. The paper contributes to the theoretical and empirical knowledge in the following way: firstly, it introduces a new approach on how governments can progressively secure e-government services; secondly, it outlines security services requirements, technical and non-technical, for maturity stages of eGMMs; and thirdly, it enhances awareness and understanding to governments and stakeholders such as practitioners, experts and citizens, regarding the importance of security services requirements being clearly defined within eGMMs stages.

5.6 Summary of Research Paper VI


My contribution: I was the main author of the paper.

Problem addressed: the goal of the study was to evaluate the proposed framework for securing e-government services which integrates IT security services into eGMMs stages [Karokola et al, 2011b].

Methodology used: The study applied qualitative as a research method and case-study as a research strategy. The strategy was applied for questionnaire preparation and data collection undertaking. In the process, evaluation methods (practical and theoretical ones) were extensively investigated and analysed, whereby a theoretical approach was chosen as a method for evaluating the proposed framework. Further, based on the literature review, seven framework evaluation criteria were developed: simplicity, coverage and completeness, compliance to security standards, and dynamics and flexibility. Other criteria were: capability and relevance, usefulness, and trustworthiness. Thereafter, a case-study with semi-structured interviews was conducted in the six government organisations studied earlier, located in Tanzania. Processing and analyses of descriptive and analytical/simple statistical data employed the use of content analysis and Microsoft excel tool respectively.

Major findings: the framework was highly accepted by the respondents in the studied organisations. Based on the acceptability ratings, among the seven evaluation criteria used to assess the framework, usefulness was rated highest at app. 95%, whilst dynamics and flexibility was rated lowest at app.76%. Further, based on the opinions given by the respondents, the framework was improved further in two ways: graphically, the framework presentation was enhanced by reducing the number of interconnections (matrix) between FIS-4 and FIS-5. Descriptively, a catalogue of security service requirements control areas (SRCAs) was enhanced with more security capabilities. Among the enhanced security capabilities were these from the Common criteria (CC) and the Systems security engineering capability maturity model (SSE-CMM).

A complete research paper is made part of this thesis in Part II. Also, the paper is in press, soon (January, 2013), it will be accessible in the proceedings of the IEEE/46th Hawaii International Conference on System Sciences (HICSS-46). Hawaii, USA.
5.7 Summary of Research Paper VII


My contribution: I was the main author of the paper.

Problem addressed: a secure electronic voting process is considered to be amongst the key factors contributing to a trustworthy, free and fair democratic election process. The goal of the study was to test the proposed framework for securing e-government [Karokola et al, 2011b] by developing a protection profile (PP) for a Controlled e-Voting System (CVS) while taking into consideration the environment of developing regions, where Tanzania was selected. Currently, Tanzania utilizes a traditional paper-based voting system.

Methodology used: An extensive literature review on protection profiles, including the Tanzanian national electoral commission documents, was performed. Further, it utilizes part of a framework for securing e-government services which integrates IT security services into e-government maturity models proposed by Karokola et al [2011b, 2012b] to develop the PP’s security services requirements, technical and non-technical. Additionally, the PP development process considered the inclusion of influencing issues for the target of evaluation (TOE) security environment, such as security threats, organizational policies and assumptions.

Major findings: the TOE security requirements areas and their rationale for the identified security threats, organizational policies and assumptions, and TOE security objectives were proposed. Having the proposed PP for e-voting system (EVS) would entail for the smooth migration from the former paper-based to the latter electronic voting system, security-wise. The study contributes to: raising levels of awareness on the importance of considering security services requirements, technical and non-technical, in electronic voting processes to governments and other stakeholders such as academia, practitioners and experts. Also, the proposed PP can be used as a checklist and baseline for guiding the procuring entity to acquire secured e-voting systems by determining the necessary security requirements and ensuring that are met; hence contributing to a trustworthy, free and fair electronic election process.

5.8 Chapter Summary

The chapter has presented extended summaries of the included research papers. The research papers were published in peer-reviewed internationally recognized (professional and academic) conferences and journals in information security and e-government. Also, the full papers are included in Part II of this thesis. All published papers contributed to the research goal. The next chapter presents concluding remarks of this research work and suggestions for future research direction.
This chapter presents the concluding remarks, research contributions, research quality and trustworthiness, and future research directions.

6.1 Concluding Remarks

The goal of this research work was to propose a framework that would facilitate government organisations to effectively offer appropriate secure e-government services. To achieve this goal four research studies were formulated along with their corresponding research questions, given in chapter 1.2. Responding to these research questions, seven research studies were conducted to cover the topic. The research was mainly guided by a design science research approach, complemented in parts by systemic-holistic and socio-technical approaches. All findings from the studies were published in peer-reviewed internationally recognised professional and academic conferences and journals in information security and e-government. The research papers are made part of this thesis as extended summaries in chapter 5 and full research papers in part II of this thesis. In addition, the summary of the research results are outlined in chapter 4, whereby a framework for securing e-government services which integrates IT security services into eGMMs was proposed.

The proposed framework attempts to bridge the current security services gap, technical and non-technical, in eGMMs by achieving measures for both quantity of e-government services and quality of security services; leading to alignment of strategic objectives between e-government services and security services – during the planning, development, implementation, service delivery and maintenance phases. Consequently, to effectively and appropriately mitigates the current and emerging security risks and threats posed to e-government services; and therefore, enhancing confidentiality, integrity and availability of critical information assets being stored, processed, and transmitted within and between e-government domains (B, C and B).

Gartner’s security technology hyper cycle suggests that the time frame for security technology to mature, normally takes between 5 to 10 years [Gartner, 2006]. Therefore, it is expected that when the proposed framework is implemented in the targeted environment it would take a similar amount of time for organisations to bridge the overall security service gap in e-government services structures, as shown in figure 6–1 below. The figure below is an extended version of figure 1–3 given in chapter 1, which suggests that the current security services gaps between e-government services sophistication will be reduced significantly over time when the framework is applied.
6.2 Research Contributions

The thesis contributes to the empirical and theoretical body of knowledge within the computer and systems sciences on securing e-government structures. It encompasses a new approach to secure e-government services, whereby a framework for securing e-government services which integrates IT security services into eGMMs was developed. The proposed framework is in line with the goal of this research work. Therefore, the main research contributions of this research work are organized as follows:

(a) Contributions to the empirical and theoretical body of knowledge is based on the following findings:

(i) Identified real-world problem in the studied environment, security issues and challenges affecting secure e-government services, reported in research papers I and II, and the identified security services (technical and non-technical) gaps in eGMMs, reported in research paper III;

(ii) Proposed maturity stages for a common frame of reference for eGMM: web-presence, interactional, transactional, transformational, and continuous improvement; reported in research paper III;

(iii) Proposed critical maturity levels of ISMM with their respective security services requirements dimensions, technical and non-technical. The security maturity levels were: undefined, defined, managed, controlled, and optimised, reported in research paper IV;

(iv) Developed a framework\textsuperscript{65} for securing e-government services, which integrates IT security services into eGMMs, along with a catalogue of

\textsuperscript{65} For instance part of this framework was used in Nepal to analyze the levels/status of e-government services and security services in the ministries. The research results were published as a Journal article [Available at http://cisjournal.org/journalofcomputing/archive/vol3no7/vol3no7_11.pdf]
security services requirements control areas (SRCAs), technical and non-technical, reported in research papers V and VI, and chapter 4;

(v) Proposed protection profile (PP) for e-voting system targeting the studied environment, reported in research paper VII. A developed PP was part of the framework testing process. Currently the studied environment (Tanzania) is still using a paper based voting system (PBVS) when conducting her national elections processes. Having the proposed PP for e-voting system (EVS) would entail smooth migration from the PBVS to EVS, security-wise, leading to trustworthiness of election processes; and

(vi) Provided a new approach for achieving secure e-government services by means of securing eGMMs. The proposed approach could be used by other researchers in the area for further enhancement.

(b) Awareness of the need for security services to be an integral part of e-government maturity models (eGMMs) and e-government services to the:

(i) Researched organizations at three different organisational levels: the strategic level (IT directors, and decision and policy makers), the tactical level (IT managers and senior personnel), and the operational level (IT technical personnel);

(ii) Different groups such as academia, practitioners, stakeholders, political leaders and policy-makers, and affected communities in general.

Figure 6–2 below places the research contribution into the information security research classification model proposed by Björck & Yngström [2001]. In the figure, the research contribution of this research, marked with a big star (*), is placed in between theories and models, and empirical world regarding level of abstraction on the y–axis, and in-between technical and formal domains on the x–axis.
6.3 Research Quality and Trustworthiness

Quality and trustworthiness of this research is based on the criteria presented by Lincoln and Guba cited in Guba [1981, pp.84–90] and Agostinho [2004, pp.9–11]. They proposed four criteria that can be used to verify the quality and trustworthiness (validity) of scientific inquiry. The criteria were: credibility, transferability, dependability, and conformability. According to Lincoln and Guba [1981] research quality and trustworthiness can be achieved through investigating the internal and external validity of research results (artifact). Whereas internal validity is associated with credibility; and external validity is associated with transferability, dependability, and conformability.

What follows is the discussion on how these criteria were achieved, in relation to this research work:

Credibility: refers to quality and validity check on whether the presented research work accurately reflects the studied reality. This research involved people, at all stages, and people are dynamic. This implies that there could be multiple realities depending on different points of view. In this case reality is limited to the context of this study. Rigor and relevance of this research work was achieved by developing an artifact (the proposed framework) that addresses the real-world problem using the rigorously research methods during the development and evaluation processes [Hevner, 2004]. The applied philosophical assumptions, theoretical foundation, research approaches, methods and strategies are discussed in chapters 2, 3 and 4, and in the published research papers. For instance, this research involved collection of suitable data by using suitable data collection instruments, use of suitable data processing and analysis techniques, and also use of triangulation and member-check techniques to ensure reliability, suitability and trustworthiness of the research results [Denzin, 1978]. Also, apart from the respondents filling in different questionnaires (data collection instruments), face-to-face interviews were conducted, and in some cases, use of recorded data. Further, the proposed framework was evaluated for internal and external validity (see chapters 2.5.4, 4.2 and research paper VI). The findings from these studies were reported in the research papers published in the peer-reviewed internationally recognised conferences and journals in information security and e-government as research papers I – VII. Therefore, this research work reflects the studied reality.

Transferability: refers to checking whether the findings from this study could be useful to other environments that shares similar conditions. Given the nature of this research work, the goal was to propose a framework that would facilitate government organisations to effectively offer appropriate secure e-government services, whereby a framework for securing e-government services which integrates IT security services into e-government maturity models was developed. Nevertheless, as it was not possible to conduct a research study in the entire area (developing regions environments), it was necessary to limit the research study to one of the developing countries where Tanzania was sampled. Within Tanzania six government organizations were selected and extensively investigated (see chapters 2.4–2.5). Hevner et al [2004] argued that an artifact (framework) that was developed for one particular environment may not
necessarily work well in another environment, simply because the underlying assumptions are different. Therefore, the findings from this research work could be replicated elsewhere in other developing countries environment that shares similar conditions.

**Dependability:** refers to whether the research findings could be repeated if the studies were to be replicated. This work is to a large extent based on the rigor theoretical foundation, research approaches, methods and strategies discussed in chapters 2 and 3. Therefore, the research findings are the result of applied rigorously research processes of inquiry that made use of suitable philosophical assumptions, research approaches, methods and strategies and theoretical foundation. Nevertheless, as reality in real-world environment keeps on changing, it may not be easy to replicate similar findings of this work elsewhere [Agostinho, 2004]. However, by establishing audit-trail\(^66\) and put more emphasis on the stability and consistency of the inquiry process may determine the dependability of the research findings of this work [Guba, 1981].

**Conformability:** refers to whether the collected data could confirm the research findings. Conformability is established when credibility, transferability, and dependability is achieved. It depends much on the objectivity of a researcher [Guba, 1981]. Data collection and analysis was based on philosophical assumptions, research approaches, methods and strategies defined in chapter 2; the theoretical foundation in information security and e-government presented in chapter 3. And the research results summarised in chapter 4, and also reported in research papers published in peer-reviewed internationally recognised conferences and journals in information security and e-government. Therefore, data collected, processed, analysed, and the reported research results in the published research papers confirm the research findings.

### 6.4 Research Limitations and Future Research Directions

The thesis has presented the suggestions on how to bridge the current security services gap in e-government services, implementation and service delivery, whereby a framework for securing e-government services was developed. The description of this section is divided into three areas: research work limitations in relation to this research, further research work to improve the framework, and other research work directions:

(a) **Research work limitations:** time constrains was the major limiting factor of this research work. As a result, some of the planned research activities were not accomplished. Un-accomplished research activities are considered for further research as described in the succeeding paragraphs. Additionally, the empirical studies in this research were limited to only one of the developing countries (Tanzania), for details see chapter 2.4.

---

\(^{66}\) Audit-trail refers to a step by step process of investigating destination and source of records that provides documentary evidence of the sequence of activities (operation, procedure, or event) performed [CC, 2009; Guba, 1981]
Further research work directions to improve the framework. The following areas are recommended for further research that would result in improving the framework. They are in line with research results reported in the published research papers:

(i) Enhancing a catalogue of SRCAs for the intermediate security maturity sub-levels: undefined, defined, managed, and controlled;

(ii) During the framework evaluation process it was observed that IT personnel at the operational level, especially those with few years of work experience in the area of information security, had difficulties to easily translate the framework SRCAs into implementations/ actions. Therefore, a further research direction should expand a catalogue of SRCAs to be more relevant to personnel at the operational level;

(iii) The framework was qualitatively (theoretically) evaluated. Further evaluation of the framework using quantitative (practical) methods is recommended, in the same environment. Furthermore, the evaluation process of the framework (theoretical and practical) could be repeated in a different environment, before generalization; and

(iv) Enhancing the capability for calculating micro economic/ financial issues for implementing security services. This capability would enable organisations to cost-effectively establish budget issues for securing e-government services.

Other research work directions. The following are possible areas for future research work directions:

(i) Bridging the perception gap between different groups within the organisations: during the evaluation process of the proposed framework, reported in chapter 4.2 and research paper VI, it was observed that there was a perception gap regarding security services adoption and use on different group levels within the surveyed organisations: strategic, tactical and operation levels. The perception gap in IT security has been observed before in Tanzania [Bakari, 2007]. Therefore, investigating on how to bridge the observed perception gap among the personnel at different organisation levels is another area that could be researched;

(ii) Inclusion of security services in e-government readiness index (ERI) survey: currently most of the conducted surveys on ERI for ICT and e-government services does not include security services surveys data. A good example is the e-government readiness index (ERI) annual survey conducted by the United Nations [2008], discussed in chapter 1. It is high time for such surveys to include security services as part of e-government readiness index. This would entail raising the levels of awareness on
security related issues, technical and non-technical, to stakeholders and responsible parties in the organisations;

(iii) *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;

(iv) *Investigate the consequences of the systemic gaps:* during the research study reported in research paper II, it was learnt that the private sector (B) appears to be an early adopter of new technology and it offers more secure services than the government sector (G). Figure 6–3 below shows a graph of e-services sophistication as a function of time, where the technology adoption and the security service gaps between the sectors B, G and C are shown. In the figure, the government sector was in the lead during the early 1990’s. Later, the private sector took the lead in adopting new technology and offering more secure services. Therefore, there seems to be a need to investigate the consequences of these systemic gaps. Should the government lead or follow?;

(v) *Outsourcing of IT security services for securing e-government services:* outsourcing is the process of, in this case, government organisations to contract out IT security services for securing e-government services (which previously have been performed internally) to IT companies (private executor). Outsourcing of IT security services is thought to improve efficiency and effectiveness of organisations (G) to provide secure e-government services to citizens (C) and businesses (B). There are many research studies conducted in the area of outsourcing IT security services. However, the research results appear to vary depending
on the studied environment. Most of the services criticism focused to privacy issues of government data being exposed to private organisations [IBM, 2003; Rowe, 2007; Tholons, 2010]. Therefore, there seems to be a need to investigate if outsourcing of IT security services in the studied environment would improve efficiency and effectiveness in offering secure e-government services. The study could also investigate the effects of adopting *cloud computing security* services [NIST, 2011], in the studied environment.
References

A


C


J


K


L


M


O


P


R


S


T


X


Y


