

**ENHANCING SECURITY OF INFORMATION SYSTEMS IN TANZANIA:
THE CASE OF EDUCATION SECTOR**

MADUHU MSHANGI

**A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN INFORMATION
SYSTEMS OF THE OPEN UNIVERSITY OF TANZANIA**

2020

CERTIFICATION

The undersigned certify that they have read and hereby recommend for examination by The Open University of Tanzania the thesis titled: **Enhancing Security of Information Systems in Tanzania: the Case of Education Sector** in fulfilment of the requirements for the degree of Doctor of Philosophy in Information Systems of The Open University of Tanzania.

í í í í í í í í í í í í í í í í í .

Dr. Edephonce Ngemera Nfuka,
(Supervisor)

í í í í í í í í í í í í í

Date

í í í í í í í í í í í í í í í í í .

Prof. Camilius Aloyce Sanga
(Supervisor)

í í í í í í í í í í í í í

Date

COPYRIGHT

No part of the thesis may be reproduced, stored in any retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the author or The Open University of Tanzania in that behalf.

DECLARATION

I, Maduhu Mshangi, do hereby declare that this thesis is my own original work and has not been presented and will not be presented to any other university for a similar or any other degree award.

í í í í í í í í í í í í í í í .

Signature

í í í í í í í í í í ..í í í ..

Date

DEDICATION

To my beloved wife Rebecca Isoso and, my lovely daughters: Salu, Joyce and Jocelyn, and my wonderful sons; Yosia and Joel.

ACKNOWLEDGEMENTS

This doctoral process has taught me much about research and the world. A journey of a thousand miles begins with a single step. Pursuing 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. I sincerely acknowledge their contributions. It is difficult and impossible to list them all here. I would like to take this opportunity to first recognize their efforts and secondly to record my deepest appreciations for their support.

I would like to thank my supervisors; Dr.Edephonce Ngemera Nfuka of The Open University of Tanzania (OUT) and Professor Camilius Aloyce Sanga of The Sokoine University of Agriculture for their unrelenting, cooperation and guidance during my study. Special thanks go to the Vice-Chancellor of The Open University of Tanzania, Professor-Elifas .T. Bisanda for facilitating the completion of my PhD. I am also indebted to the Office of the Deputy Vice-Chancellor (Academic) and Postgraduate coordinator office for the advice, starting from the registration process to the completion of this thesis. I am indeed grateful to the Dean of the Faculty of Science, Technology & Environmental Studies, and the ICT department at OUT for making this dream to happen. Additionally, special thanks go to Dr. Chacha Matoka of OUT for encouraging me to pursue the PhD Programme at OUT.

I am also grateful to the National Examinations Council of Tanzania (NECTA) for granting me permission to undertake my studies. I, however, wish to specifically acknowledge H.E. Professor Joyce Ndalichako, currently the Minister for Education, Science, and Technology, who was then the Executive Secretary of NECTA at the

time I started my dream journey of pursuing PhD for study leave permission. Many thanks go to Dr. Charles E. Msonde- who is currently the Executive Secretary of NECTA for granting study permission and for his encouragements that made it possible to finalize my PhD study. My thanks to all heads of departments, sections, and all NECTA employees. Special thanks go to Dr. Joseph Mbowe, head of ICT department at NECTA and Mr Hassan Kondo who was acting head of the ICT department at NECTA at the time of starting my PhD journey for their encouragement. Special thanks go to Mr Augustine Mtika, Mr Limbu M. Limbu and Mr Japhet Guyai for their corporation during prototyping development and pilot testing. Special thanks to my co-workers at NECTA in a Systems Administrations and Security Section for their cooperation namely: Mr Mahamud Tamatamah, Mr Prospective Gikanka, Mr Kehongo Jacob, Ms Perusi Ryoba and Mr Augustine Mtika.

Finally, nothing that I would have been possible throughout the period of my study was it not the constant support, faithfulness, patience, and love of my wife- Rebecca Isoso. I wish to thanks my lovely daughters- Salu, Joyce and Jocelyn; my lovely sons - Yosia and Joel, for their patience, understanding, and love during the study. May God showers his blessing to all who contributed to the completion of the study.

ABSTRACT

The ICT initiatives and ICT use are on the rise across the global including the education sector in Tanzania. Departments, agencies, authorities, and ministries responsible for education in Tanzania have deployed information systems for delivering e-services. The focus is on ICT use in which security concern has not been fully put into consideration. Information systems (IS) are being deployed without incorporating fully security requirements during systems development lifecycle (SDLC). This result in deployed IS to be insecure. The study adopted mixed research methods, quantitative and qualitative. The study assessed and identified appropriate security requirements (security measures and security controls) for ensuring security goals (confidentiality, integrity and availability) of information in IS. It employed ISO/IEC 21827: Systems Security Engineering-Capability Maturity Model (SSE-CMM) to assess the security maturity in IS, a case study of the education sector in Tanzania. It established the security status quo research gap for improvement and developed a multi-layered security framework for enhancing the security of IS. The study used field experiments in the education sector and employed cryptographic algorithm-based techniques to validate the developed framework. The framework was further evaluated for its performance, perceived ease of use and perceived usefulness in improving the security of IS. The developed multi-layered security framework can be employed in a real-world environment to enhance the security of IS. The proposed solution can be extended to other sectors with similar security requirements.

TABLE OF CONTENTS

CERTIFICATION.....	ii
COPYRIGHT	iii
DECLARATION	iv
DEDICATION	v
ACKNOWLEDGEMENTS.....	vi
ABSTRACT	viii
TABLE OF CONTENTS.....	ix
LIST OF TABLES.....	xiv
LIST OF FIGURES	xxii
ABBREVIATIONS AND ACRONYMS.....	xxiv
CHAPTER ONE	1
INTRODUCTION	1
1.1 General Introduction.....	1
1.2 Statement of the Problem	9
1.3 Research Objectives	10
1.4 Research Questions	11
1.5 Research Process	11
1.6 The Significance of the Study.....	13
1.7 Research Scope	14
1.8 Thesis Report Organization	14
CHAPTER TWO.....	15
LITERATURE REVIEW.....	15
2.1 Introduction.....	15

2.2	Information Systems Security.....	15
2.2.1	Security Goals.....	17
2.2.2	Security of Assets.....	26
2.3	Enhancing Security of Information Systems	28
2.3.1	Security Models, Frameworks and Standards.....	28
2.3.2	Security Standards and Best Practices.....	34
2.3.3	Security Domains	35
2.4	Soft Systems Methodology and Design Science Research	36
2.4.1	Soft Systems Methodology.....	36
2.4.2	Design Science Research.....	37
2.5	Related Work	37
2.5.1	Security Measures for Ensuring Security Goals	40
2.5.2	Security Controls.....	50
2.6	Research Gap	58
2.7	Conceptual Framework	60
	CHAPTER THREE.....	63
	RESEARCH METHODOLOGY.....	63
3.1	Introduction.....	63
3.2	Research Paradigms	63
3.2.1	Soft System Methodology	63
3.2.2	Design Science Research.....	66
3.2.3	Integrating SSM withDSR.....	70
3.3	Research Methods	72
3.4	Problem Relevance and Root Definition	74

3.5	Research Design.....	77
3.5.1	Study Area	77
3.5.2	Organizations under Study	78
3.5.3	The Sampling Design	79
3.5.4	Data Collection Techniques.....	80
3.5.5	Designing of Survey Questionnaires.....	83
3.5.6	Design of Interview Data Collection Matrix Tool.....	85
3.5.7	Pre-Testing and Pilot Study	85
3.6	Access and Research Ethics.....	85
3.7	Data Analysis	85
3.7.1	Data Analysis Techniques	85
3.7.2	Statistical Data Analysis of Collected Data.....	87
3.8	Validity and Reliability	89
	CHAPTER FOUR	91
	FINDINGS	91
4.1	Introduction.....	91
4.1.1	General Introduction.....	91
4.1.2	Overview of Data Analysis.....	91
4.2	Security Measures for Ensuring Security Goals	94
4.2.1	Measures for Ensuring Confidentiality of Information.....	94
4.2.2	Measures for Ensuring the Integrity of Information	114
4.2.3	Measures for Ensuring Availability of Information.....	129
4.3	Security Controls and Security Domains.....	142
4.4	Improving the Security of Information and Information Systems	215

4.4.1	Security Actions for Improving Security of Information Systems	215
4.4.2	Challenges and Security Incidents Affecting Information Systems	217
4.4.3	Institutional Maturity Comparisons	219
4.4.4	Security Domains Maturity Comparisons	220
CHAPTER FIVE		225
DISCUSSION OF THE FINDINGS		225
5.1	Introduction.....	225
5.2	Security Measures for Ensuring Security Goals	225
5.2.1	Security Measures for Ensuring Confidentiality of Information	226
5.2.2	Security Measures for Ensuring the Integrity of Information.....	234
5.2.3	Security Measures for Ensuring the Availability of Information	240
5.3	Security Controls and Security Domains	247
5.4	Framework For Enhancing Security of Information Systems	263
5.4.1	Requirements for Developing Framework for Enhancing Security of Information Systems.....	264
5.4.2	Developed framework for Enhancing Security of Information Systems	268
5.5	Human Sensor Web Prototype for Crowdsourcing Security Incidents.....	277
5.6	Validation of the Developed Framework using Cryptographic Techniques	280
5.6.1	Security Requirements for Ensuring Security of Information and Information Systems using Cryptographic Techniques	282
5.6.2	Algorithm for Enhanced Security of Information Systems Using Cryptographic Techniques.....	286

5.6.3	Illustration of Developed Algorithm for Enhanced Security.....	288
5.6.4	Performance Analysis of The Developed Algorithm For Enhanced Security Based on Cryptographic Techniques Using a Controlled Experiment.....	290
5.6.5	Discussion of the Validation of the Developed Framework for Enhancing The Security Of Information	297
5.7	Evaluation of the Framework for Enhancing the Security of Information Systems.....	298
5.8	Discussion of the Evaluation of the Developed Framework for Enhancing Information Systems Security	309
CHAPTER SIX.....		312
CONCLUSION AND RECOMMENDATIONS.....		312
6.1	Conclusion	312
6.1.1	Research Summary.....	312
6.1.2	Answers to Research Questions	314
6.1.3	Research Contributions	317
6.1.4	Limitations and Further Research Work	319
6.2	Recommendations	319
REFERENCES		320
APPENDICES.....		356

LIST OF TABLES

Table 1.1: Information Systems in the Education Sector in Tanzania	6
Table 3.1: Applying Design Science Compounded With Soft Systems	
Methodology	66
Table 3.2: Comparison of Design Science Research and Soft Systems	
Methodology	70
Table 3.3: Integrating Soft Systems Methodologywithdesign Science Research	71
Table 3.4: Description of the Organizations Under Study.....	78
Table 3.5: Respondents.....	80
Table 3.6: Summary of an interview data sample	82
Table 3.7: Document review	83
Table 3.8: SSE-CMM Rating Scale Description.....	84
Table 4.1: Research Questions and Data Collection Tools Mapping.....	92
Table 4.3: Unique User Account And Password for Accessing	
Information Systems.....	96
Table 4.4: Smartcards for Accessing Information Systems.....	97
Table 4.5: Physical lock keys and smartcards/biometric	98
Table 4.6: Technologies to Block or Restrict Unencrypted Sensitive Data	100
Table 4.7: Classifying Information Resources: Public, Confidential, Secret	101
Table 4.8: Access Control Mechanism: Authorizing And Revoking Access	102
Table 4.9: Network Segmentation: Subnets, VLAN	103
Table 4.10: Protecting servers by more than one security layer	105
Table 4.11: Encryption of Data During Transmission/Processing	106

Table 4.12: Encryption of Data During Storage..... 107

Table 4.13: Media-Sanitization: Destroy Data Permanently 108

Table 4.14: Insecure Services, Protocols, and Ports..... 110

Table 4.15: Updates or Patches: Antivirus/OS..... 111

Table 4.16: IT Staff Security Awareness and Training 113

Table 4.17: Logging, Monitoring Logs and Alerting 114

Table 4.18: Review Administrative Account and Operative Access to
 Audit Logs 116

Table 4.19: Prevent Unauthorized Access and Tempering of System Logs..... 117

Table 4.20: Encryption and Digitally Signing Of Messages..... 118

Table 4.21: Checksum 119

Table 4.22: Job Rotation 120

Table 4.23: Segregation of Duties 121

Table 4.24: Change management for information systems..... 123

Table 4.25: Automatically logging of changes 124

Table 4.26: Audit Logs for Sensitive Information 125

Table 4.27: Monitor Wired (LAN/WAN) And Wireless Networks..... 126

Table 4.28: Integrity monitoring tool 128

Table 4.29: Procedures to Review Users' Access..... 129

Table 4.30: Business continuity plan..... 131

Table 4.31: Incident Management and Response..... 133

Table 4.32: Incident Response Team Aware Of Legal Or Compliance
 Requirements 134

Table 4.33: Disaster Recovery Plan..... 135

Table 4.34: Backup Strategies.....	136
Table 4.35: Data Backup Process.....	137
Table 4.36: Test of Restore Procedures.....	138
Table 4.37: Sufficient capacities	139
Table 4.38: Fault Tolerance	140
Table 4.39: Systems Monitoring Mechanisms.....	141
Table 4.40: Preventative Measures to Protect Critical Hardware and Wiring.....	142
Table 4.41: Summary Results for Information Security Policy Controls.....	144
Table 4.42: Information Security Policy Approved	145
Table 4.43: Information Security Policy Published and Communicated.....	147
Table 4.44: Information security policy reviewed	149
Table 4.45: Summary results for organizational information security	150
Table 4.46: Security Responsibility.....	151
Table 4.47: Information Security Committee	152
Table 4.48: Signing Terms and Conditions: Responsibilities for Security.....	152
Table 4.49: Budget: information security program	153
Table 4.50: Signing Confidential or Non-Disclosure Agreement	154
Table 4.51: Summary Results for Human Resources Security	155
Table 4.52: Screening, Background Checks	156
Table 4.53: Security Awareness, Training, and Education.....	158
Table 4.54: Security Awareness Training.....	159
Table 4.55: Specialized Role-Based Training.....	159
Table 4.56: Information security programs.....	160
Table 4.57: Revoking System Access on Termination.....	161

Table 4.58: Revoking system access when there are a change of roles	162
Table 4.59: Disciplinary Action: Non-Compliant With Information Security Policy	162
Table 4.60: Summary results for asset management	164
Table 4.61: Identification of Critical Information Assets	165
Table 4.62: Classifying information resources - assets	165
Table 4.63: Summary Results for Access Controls	167
Table 4.64: Access control policy	168
Table 4.65: Rules/Policy For Using IS	169
Table 4.66: Access Control Policy for Authorizing And Revoking Access Rights.....	169
Table 4.67: Process in Place for Granting and Revoking Appropriate User Access.....	170
Table 4.68: Password Management Program.....	171
Table 4.69: Procedures to Regularly Review Access	171
Table 4.70: Securing of Remote Access	172
Table 4.71: Prevent and Detect Rogue Access to Wireless-LANs	173
Table 4.72: Restrict Unencrypted Sensitive Information to Untrusted Networks ...	173
Table 4.73: Restrict the Sharing of Passwords.....	174
Table 4.74: Authorization System That Enforces Time Limits Lockout On Login Failure.....	175
Table 4.75: Policies and Controls for The Use Of Mobile Devices	175
Table 4.76: Encryption of Mobile Computing Devices.....	176
Table 4.77: Telework policy	177

Table 4.78: Cryptography Controls	178
Table 4.79: Summary Results for Physical and Environmental Security.....	179
Table 4.80: Physical and Environmental Security Policy.....	180
Table 4.81: Restrict Physical Access to A Sensitive Area.....	180
Table 4.82: Protection of Critical Hardware and Wiring.....	181
Table 4.83: Background Checks for Access to Sensitive Facilities	181
Table 4.84: Media-Sanitization Process	182
Table 4.98: Summary Results for Communication Security Controls	183
Table 4.99: Network Security Policy.....	184
Table 4.100: Segmented Network Architecture	185
Table 4.101: Internet-Accessible Servers Are Protected.....	185
Table 4.102: Appropriate Encryption Methods to Protect Sensitive Data in Transit.....	186
Table 4.103: Policies and Procedures to Protect The Exchange of Information	187
Table 4.104: Protecting E-Commerce Data Traversing Public Networks.....	187
Table 4.105: Summary Results for System Acquisition, Development and Maintenance	188
Table 4.106: Acquisition, development and maintenance policy	190
Table 4.107: New IS or enhanced IS security requirements validation	190
Table 4.108: Standards that address secure coding practices	191
Table 4.109: Validation Checks to Ensure Data Output is as Expected.....	192
Table 4.110: Policies to Indicate When Encryption Should be Used.....	192

Table 4.111: Configuration Management Process for Changes to its Critical Systems	193
Table 4.112: Perform Reviews and Tests to Changes Made to Production Systems	194
Table 4.113: Security Requirements for Outsourced Software Development	194
Table 4.114: Patch Management For Monitoring And Responding to Patch Releases	195
Table 4.115: Policies, Procedures for Managing Suppliers Relationships	196
Table 4.116: Incident Handling Policies and Procedures Throughout its Life Cycle	198
Table 4.117: Summary Results for Operation Security	198
Table 4.118: Change Management Policy and Acceptable Use Policy	200
Table 4.119: Security Configuration Standards for IS and Applications	201
Table 4.120: Changes to IS are Tested, Authorized And Reported	201
Table 4.121: Duties are Sufficiently Segregated	202
Table 4.122: Production Systems are Separated from Other Stages	202
Table 4.123: Monitor The Utilization of Key Systems Resources	203
Table 4.125: Methods for Detecting and Eradicating Known Malicious Code	204
Table 4.126: Backup Procedures	205
Table 4.127: Routine Test of Restore Procedures	205
Table 4.128: Logging Automatically Security-Related Activities	206
Table 4.129: Routinely Monitoring of Logs	207
Table 4.130: File-Integrity Monitoring Tools for Alerting	208
Table 4.131: Business Continuity Plan Controls	209

Table 4.132: Summary Results for Compliance Controls	210
Table 4.133: Evaluation of Compliance With Security Policies and Standards	211
Table 4.134: Application and Network Layer Vulnerability Orpenetration Testing	211
Table 4.135: Summary Results for Risk Management Controls.....	212
Table 4.136: Risk Management Program and Risk Register	213
Table 4.137: Risk Register Reviewed and Updated	214
Table 4.138: Conducts Routine Risk Assessments	214
Table 4.139: Desk Document Review	216
Table 4.140: Challenges, Incidents Affecting Information Systems/E-Services	217
Table 4.141: Summary of Security Domain Assessed for the Maturity Level	220
Table 4.142: Security Domains Maturity Level.....	221
Table 5.1: Security measures for ensuring information states confidentiality.....	234
Table 5.2: Security measures for ensuring the integrity of the information	240
Table 5.3: Security Measures for Ensuring The Availability of Information	247
Table 5.4: Summary of Security Controls and Security Domains	258
Table 5.5: Security Measures for Ensuring Security Goals	274
Table 5.6: Algorithm for Enhanced Security Using Cryptographic Techniques	287
Table .5.7: Classes for a Prototype For Illustrating an Algorithm for Enhancing Security.....	289
Table 5.8: Enhancing Security During Storage in IS Using Crypto Techniques	295
Table 5.9: Results of Execution Time For A Simulation Experiment.....	295

Table 5.10: Evaluating the Performance: Perceived Ease Of Use	302
Table 5.11: Evaluating the Perceived Usefulness	303
Table 5.12: Elements of the Developed Framework are Clear And Helpful.....	306
Table 5.13: Framework for Enhancing the Security of IS Is Easy to Use.....	307
Table 5.14: Skillful at Using The Developed Framework.....	308
Table 5.15: Developed Framework Would Improve The Security of Information systems	309

LIST OF FIGURES

Figure 1.1: Research Process for Enhancing the Security of Information Systems.....	12
Figure 2.1: Conceptual Framework for Enhancing Security of Information Systems.....	62
Figure 3.1: Stages of soft systems methodology.....	64
Figure 3.2: Soft Systems Methodology Integrated With Design Science Research.....	65
Figure 3.3: Design Science Research Cycles.....	68
Figure 3.4: Soft Systems Integrated with Design Science Research.....	72
Figure 3.5: Root Problem Definition.....	76
Figure 3.6: Soft Systems Methodology integrated with Design Science Research ...	86
Figure 4.1: Institutional Maturity Level in SSE-CMM	220
Figure 4.2: Line Graph For Security Domain Maturity Level.....	223
Figure 4.3: Radar for Institution security domain maturity	224
Figure 5.1: Proposed Authentication an Authorization System Architecture.....	227
Figure 5.2: Crypto System Architecture for Ensuring Confidentiality of Information and Information Systems.....	232
Figure 5.3: Cryptographic Systems Architecture for Enhancing the Integrity of Information And Information Systems.....	236
Figure 5.4: High Availability Distributed Systems Architected Integrated With CDN	244
Figure 5.5: Information Systems Security Interrelations of Components	267
Figure 5.6: Framework for Enhancing the Security of Information Systems	269

Figure 5.7: Security System Architecture For Validating the Framework For Enhancing The Security Of Information Systems Using Cryptographic Techniques.....	284
Figure 5.8: Snapshots of Java Classes For Developed Algorithm For Enhanced Security	289
Figure 5.9: Execution Results For Enhancing Security During Transmission in IS.....	292
Figure 5.10: Encrypted Results in Table Fields During Storage in IS	294
Figure 5.11: Results Execution Time For Enhancing Security During Transmission in IS.....	296
Figure C.1: Logical Schema for Data Capturing Tool	372

ABBREVIATIONS AND ACRONYMS

CIA	Confidentiality, Integrity, and Availability
CMM	Capability Maturity Model
DSR	Design Science Research
DSRP	Design Science Research Paradigm
HERIN	Higher Education Research Institutions Network
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
IS	Information Systems
ISO	International Organization for Standardization
ISO/IEC:21827	Information technology - Security techniques -Systems Security Engineering-Capability Maturity Model (SSE- CMM)
ISO/IEC 27001	Information technology -Security techniques - Information security management systems ó Requirements
ISO/IEC 27002	Information technology -Security techniques - Code of Practice for information security management
ISS	Information systems security
IT	Information technology

CHAPTER ONE

INTRODUCTION

1.1 General Introduction

Information and communications technologies (ICT) is a tool and enabler for enhancing education delivery, processes, outcomes and impact (URT, 2017). It is an infrastructure and a strategic agent for economic change transformation (Cunningham & Cunningham, 2017). It is a motive and driving force for transforming the economy of Tanzania into a knowledge-based economy and middle-income country by 2025 (URT, 2017). The adoption of ICT in Tanzania can be looked at from the first computers used at the Ministry of Finance in 1965 (Lubua & Maharaj, 2012).

The importation of computers and related ICT equipment was banned in 1974 due to the failure of accounting information system implementation at the Ministry of Finance (Mgaya, 2010; Lubua & Maharaj, 2012). The importation of computers was later on allowed (Mgaya, 2010; Lubua & Maharaj, 2012). The Government established National ICT policy 2003 to govern ICT in Tanzania; which has been updated to National ICT policy 2016; the following is a review (URT, 2003, 2017). Moreover, the Government has enacted the Cybercrime Act 2015 (URT, 2015a) and the Electronic Transactions Act 2015 (URT, 2015b) to govern the security and electronic transactions in the country. Additionally, the education sector in Tanzania has formulated ICT policy for basic education in 2007 (URT, 2007) to govern the use of ICT in the education sector (MEST, 2016).

ICT Initiatives are currently ongoing at the national level in the areas of e-

Infrastructure and Education (Science, Technology and Higher Education Program, Tanzania National Research and Education Network, e-Libraries, Education Management Information System). Another initiative is in the areas of e-Health, Information Society and Entrepreneurship (TANZICT project, Dar Teknohama Business ICT Incubator, Binu Innovation Hub) and the Tanzania ICT Technology Park (Cunningham & Cunningham, 2017). Another remarkable project is the Government electronic payments gateways (GePG) for integrating all payments in the Government (URT, 2019) including education sector in Tanzania.

The education sector is vital for the socio-economic development of individuals, communities, and societies in Tanzania (MEST, 2016; URT, 2017). It is governed by the Ministry of Education, Science, and Technology; and the President's Office Regional Administration and Local Government (MEST, 2016; PMO-RALG, 2016). A number of initiatives are going on for the use of ICT and integration in the education sector from pre-primary, primary and secondary to tertiary education in Tanzania. The investment landscape of ICT use in the education sector in Tanzania is on the rise (MEST, 2016; Cunningham & Cunningham, 2017). This can best be viewed through different ICT initiatives.

The Ministry of Education Science and Technology (MEST) has deployed an ICT project to more than 34 teachers colleges for e-learning and m-learning. Additionally, the Government has deployed optic fibre ICT infrastructure to districts and municipalities across the country to facilitate ICT use in the education sector in Tanzania (Cunningham & Cunningham, 2017). Moreover, various information

systems (IS) have been deployed at ministries responsible for education, agencies, departments, and commissions in the education sector in Tanzania. The MEST has developed interactive web portal where citizens and various stakeholders can interact with to get various information such as to search for a school on educational management information systems database to see registration status and where located, get answers to commonly asked questions, online help-desk (MEST, 2016).

MEST has further launched a project for the use of ICT in secondary schools across the country in collaboration with Global e-schools and Communities Initiative (GeSCI) (THE CITIZEN, 2017). The project was launched in October 2017 for using ICT for learning and teaching in secondary schools. The project initial investment was 4billion Tanzania shillings for Morogoro and Coastal region. It focuses on Science, Mathematics and English subjects (ITNEWSAFRICA.COM, 2017) for ICT use in education assessment (teaching and learning). Thus, it will transform secondary schools in Tanzania into the digital education system.

Moreover, agencies, departments, commissions, institutions such as universities and colleges have taken various ICT initiatives (Table 1.1) such as central admission systems have been deployed by Tanzania Commission for Universities (TCU) and National Council for Technical Education (NACTE). The online loan application system has been deployed by Higher Education Students' Loans Board (HESLB) for facilitating loan applications, processing and allocation of loans to students in higher learning institutions (universities and colleges for degree courses and some diploma courses). Online application and admission systems at colleges and universities have

been deployed. Electronic services systems integrated with GePG (URT, 2019), online registrations systems, educational assessment systems for capturing continuous assessments at school levels and colleges have been deployed by the National Examinations Council of Tanzania (NECTA) in collaboration with ministries responsible for education.

Additionally, NECTA in collaboration with the ministries responsible for education has implemented a centralized application program interface (API) system for online verification of examinations results (NECTA, 2019). It is used for students' admission applications from various higher learning institutions in Tanzania. The systems from higher learning institutions perform real-time online verification of examinations results without manual intervention through NECTA API centralized repository.

Moreover, NECTA in collaboration with ministries responsible for education has deployed a unique identification number for tracking student progress from primary school and other education levels like colleges and universities. This unique identification number can be used to link with other IS in Tanzania like Registration Insolvency and Trusteeship Agency (RITA) database (for birth and death registration), National Identification Authority (NIDA) database (for national ID), and Tanzania electronic passport system database.

All these ICT initiatives in the education sector in Tanzania are going without investment in security for deployed information systems and ICT. Information

systems (IS) are comprised of software-hardware, databases, networks, operations procedures and people (Whitman & Mattord, 2012). IS have different information states namely capturing, processing, storage and transmission state. Security of information is concerned with ensuring security goals (confidentiality, integrity and availability) (Bosworth et al., 2014) during information states in IS.

Security begins at the top and everyone should be concerned with the security of information in IS at all stages from initiation of the project to deployment (Bakari, 2007; Shaaban, 2014). It should be incorporated in all business processes including its inputs and outputs. However, the security of information in IS are too often regarded as an afterthought in the design and implementation of IS (Bosworth et al., 2014). In fact, the importance of security must be felt and understood at all levels of command and throughout the education sector (Karakola, 2012; Shaaban, 2014). The culture of security is required throughout the education sector. Education sector keeps on investing in the ICT use for e-services delivery without much consideration of the security of information in IS from initial conceptualization to the implementation.

The investment of ICT for e-services delivery across the globe and education sector, in particular, has created security challenges on how to ensure security goals (confidentiality, integrity and availability) of information in IS hosted in cyberspace, ubiquitous computing environment (Jang-Jaccard & Nepal, 2014; URT, 2015a; Symantec, 2017). The education sector in Tanzania has computerized some of the

services which were manually offered to e-services. Table 1.1 presents some of the e-services offered to citizens in Tanzania and different stakeholders across the globe.

Table 1.1: Information Systems in the Education Sector in Tanzania

S/N	Institutions	Information systems (e-services)	Secure protocols
1	National Council for Technical Education (NACTE): www.nacte.go.tz	-Central Admission System -Online Awards Evaluation System	https and security token authentication
2	Tanzania Commission for Universities (TCU): www.tcu.go.tz	-Central Admission System (CAS) -Program Management System(PMS) -Foreign Award Assessment System(FAAS) -Commission Resolution Management System (CRMS) -Exhibitions participation registration portal	https, security token authentication
3	Higher Education Students' Loans Board (HESLB): www.heslb.go.tz	Online loan application & management system	https, identity and authentication: user ID, password and SMS/e-mail code authentication
4	National Examinations Council of Tanzania(NECTA): www.necta.go.tz	-NECTA Online registration system -NECTA portal & SMS results disbursement system -NECTA application program interface (API) system for online verification of examinations results in higher learning institutions in Tanzania	https, security token authentication for API
5	Ministry of Education, Science, and Technology (MEST): www.moe.go.tz	-MEST Portal, -An electronic sel-form system, -Education management information system (EMIS).	https, identity and authentication: user ID, password
6	Tanzania Institute of Education (TIE): www.tie.go.tz	TIE Portal	https; identity and authentication: user ID, password
7	Institute of Adult Education(IAE): www.iae.ac.tz	IAE Portal	https; identity and authentication: user ID, password
8	Tanzania Library Services Board (TLSB): www.tlsb.or.tz	TLSB Portal, Library Information system	https; identity and authentication: user ID, password
9	Agency for the Development of Educational Management(ADEM): www.ademtz.com	ADEM Portal	https; identity and authentication: user ID, password
10	Vocational Education and Training Authority (VETA): www.veta.go.tz	VETA Portal and VETA mobile learning system	https, SMS code authentication
11	Tanzania Education Authority (TEA): www.tea.or.tz	TEA Portal	https; identity and authentication: user ID, password

S/N	Institutions	Information systems (e-services)	Secure protocols
12	President's Office Regional Administration and Local Government (PORALG): http://www.tamisemi.go.tz	-PORALG Portal -Form Five selection system	https; identity and authentication: user ID, password

Source: field data, 2017

These e-services are mainly offered through mobile and web-based IS in cyberspace (Johansson, 2014; Sur & Yazici, 2017). The trend of hosting IS in cyber-space such as Internet and cloud computing has created challenges in maintaining security, due to increases of cybercrimes in the globe (Jang-Jaccard & Nepal, 2014; Kaspersky, 2017; Symantec, 2019). The rapid growth of cybercrimes and increased cyber-attacks (Nfuka et al., 2014) happening globally have been accelerated by the increased Internet users and mobile value-added services (such as M-Pesa, Tigo-Pesa, Airtel Money, EzyPesa, Halotel Money) integrated into IS (Yonazi, 2012; TCRA, 2017). The increase in the number of Internet and mobile users has a direct implication to the increase in cybercrimes affecting IS around the globe including education sector (Jang-Jaccard & Nepal, 2014; Nfuka et al., 2014; Symantec, 2019).

An earlier study by Nfuka et al. (2014) revealed that 12.8% of users in the education sector in Tanzania experience cyber-attacks due to visiting unhealthy websites; 63.29% of e-mails received by users are spam. Furthermore, many websites and IS in the education sector in Tanzania have been hacked within the period of less than a month interval in 2017. These include hacking of The Open University of Tanzania website, hacking of the University of Dar es Salaam; hacking of the TCU web-based information system in 2017 (Jamiiforums, 2017; Mwananchi, 2017). This trend of hacking of IS in cyberspace by exploiting vulnerabilities (open security holes) is on the rise as ICT advances with time (Kaspersky, 2017; Symantec, 2019).

The vulnerabilities and design flaws in IS are the consequences of misconfigurations (software or hardware) and insecure coding practices (Bosworth et al., 2014; Wang et al., 2018). The insecure coding (OWASP, 2017) is the failure to incorporate security requirements (security measures and security controls) during the systems development life cycle (SDLC). The misconfigurations include human error, enabling debug error mode in applications, running outdated software, unnecessary services, misconfigured SSL, disabling security settings, improperly authenticated IS, default installations (using default settings, default passwords) (Shamsi & Khojaye, 2018). Furthermore, attacks are the results of buffer overflows (causing DoS/DDoS); unpatched IS (servers, operation systems (OS), applications, and firmware); design flaws (incorrect encryption, poor validation, logical flaws, OS flaws, applications flaws); and open services (OWASP, 2017; Wang et al., 2018). These cause security holes in IS which can be exploited by attackers.

The exploitation of security holes causes a violation of security goals (loss of confidentiality, integrity and availability) for information in IS. The problem of violation of security goals can be addressed by identifying, assessing and implementing effective security measures and security controls for ensuring security goals (confidentiality, integrity and availability) of information in IS during information states in IS. This problem is mainly contributed by a human factor as the weakest link in the security chain (Bosworth et al., 2014).

1.2 Statement of the Problem

The ICT initiatives are ongoing in the education sector as technology advances across the global. Departments, agencies, authorities, and ministries responsible for education in Tanzania (Ministry of Education, Science and Technology; and President's Office-Regional Administration and Local Government) have initiated various e-services. These ICT initiatives are fragmented with duplication of efforts. The technical advances in ICT do not always ensure the security of IS. Moreover, their focus was on ICT use; security of IS has not been taken into consideration. Systems are developed and deployed without incorporating security requirements in each stage of SDLC. This results in insecure IS with open holes (vulnerabilities). The vulnerabilities in IS are the consequences of misconfigurations (software or hardware) and insecure coding (failures to incorporate security requirements during SDLC)(Bosworth et al., 2014; Wang et al., 2018). These cause exploitable security holes leading to threats/risks to IT assets.

Attackers exploit these vulnerabilities to perform various attacks on IT assets. This results in loss of confidentiality, integrity and availability of information in IS. The existing ICT security management guidelines to combat these attacks are inadequate. They lack a comprehensive security framework for assessing, identifying, and incorporating security requirements (security controls and security measures) to ensure security goals for IS. There is no comprehensive security framework which addresses the issue of failure to ensure security goals of information in IS. The institutions/organizations (or sector) for delivering e-services, requires a comprehensive security framework for building secure IS. The comprehensive

security framework assists in assessing, identifying and integrating security requirements in each stage of SDLC. The failure to incorporate security requirements during SDLC results in cyber-attacks.

Cyber-attacks across the globe, including the education sector in Tanzania, are on the rise (Jang-Jaccard & Nepal, 2014; Kaspersky, 2017; Symantec, 2019). A study by Nfuka, *et al.* (2014) found that 12.8% of users experience cyber-attacks through accessing higher risks websites; 63.29% electronic mails received are spams e-mails in the education sector in Tanzania. Moreover, 89% of IS in the education sector in Tanzania are vulnerable to cyber-attacks (Jang-Jaccard & Nepal, 2014; Mshangi *et al.*, 2015; Chand & Mathivanan, 2016). These cyber-attacks lead to loss of security goals (confidentiality, integrity and availability) of information in IS. Thus, the research problem was the loss of confidentiality, integrity and availability of information in IS, case of the education sector in Tanzania.

1.3 Research Objectives

1.3.1 Main Research Objective

The main objective of this study was to assess security requirements and develop a framework for enhancing the security of information systems in Tanzania: the case of the education sector.

1.3.2 Specific Objectives

The specific objectives of this study were:

- i. To assess the existing security measures for ensuring confidentiality, integrity, and availability of information in information systems

- ii. To assess the existing security controls for ensuring the security of information in information systems
- iii. To develop a framework for enhancing the security of information systems
- iv. To validate the developed framework for enhancing the security of information systems
- v. To evaluate the developed framework for enhancing the security of information systems

1.4 Research Questions

The research questions for this study were:

- i. To what extents are the existing security measures ensure confidentiality, integrity and availability of information in information systems?
- ii. To what extents are the existing security controls ensure the security of information in information systems?
- iii. How to develop a framework for enhancing the security of information systems?
- iv. How to validate the developed framework for enhancing the security of information systems?
- v. How to evaluate the developed framework for enhancing the security of information systems?

1.5 Research Process

Figure 1.1 depicts the research process in this study. It comprises of series of steps namely - define the research problem (problem statement), main research objective, specific research objectives, research questions, literature review, research gap, conceptual framework, research methodology (design research, sampling design,

data collection tools, research methods), data collection, data analysis, findings, discussions of findings, framework development for enhancing security of IS, development of the prototype, evaluation of developed framework, research contributions, and conclusions and recommendations. The research process (Figure 1.1) was managed by soft systems methodology (Checkland, 1998) compounded with design science research (Hevner *et al.*, 2004) executed in an iterative systematic circular fashion until the optimal value was reached in each step in the research process.

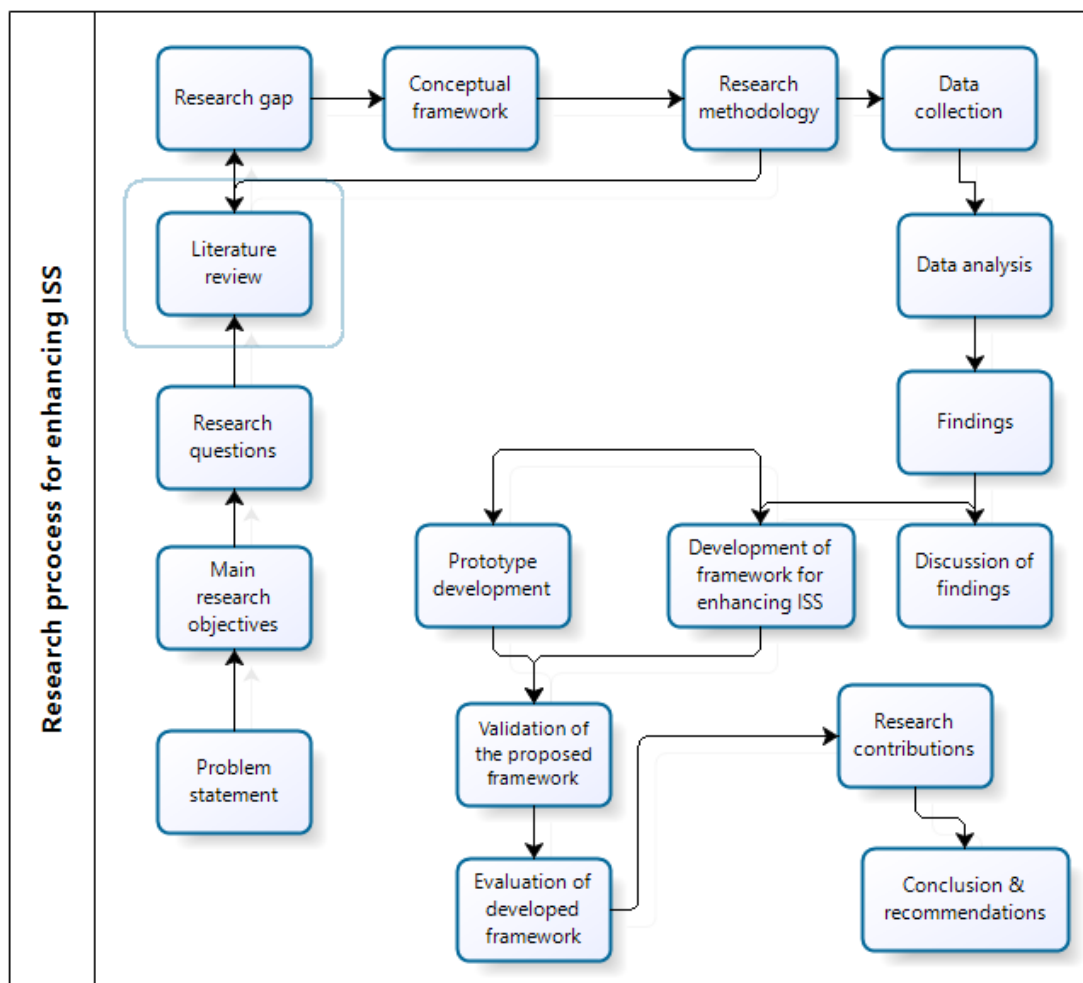


Figure 1.1: Research Process for Enhancing the Security of Information Systems

1.6 The Significance of the Study

The significance of this study was to enhance the security of IS in the education sector for effective delivery of both formal and informal education. This is consistent with ICT Education Policy, 2007 and National ICT Policy, 2016 which pointed out that there is a need to create a secure electronic learning environment. This was achieved by addressing the problem of failure to ensure security goals for IS. The study developed a framework for enhancing the security of IS. Furthermore, the study developed a human sensor web for crowdsourcing information related to security incidents management in the education sector. This creates a favourable environment for the secure use of ICT by different stakeholders in the education sector in Tanzania. This enables teachers, students and different stakeholders to share and exchange information and knowledge in a secure way (by guaranteeing security goals).

The significance of this research to the Government is that different findings have direct input to the ICT policymakers and implications in the country especially in the area of information systems security. For example, the findings have direct inputs for the creation of new law(s), policies and amendment of existing policies and ACTS such as The Cybercrimes ACT, 2015 to recognize whistleblowers. Moreover, the study has a contribution to the academic field as the findings from this research can be used for reference purposes in the process of teaching/learning. Researchers can also use the findings as inputs to various future researches.

1.7 Research Scope

The study scope was to assess security measures, and security controls for ensuring the security of information in IS, and develop a framework for enhancing the security of information systems, a case study of education sector in Tanzania. It assessed security requirements to find out the status quo research gap for taking action to enhance the security of information in IS. It developed a multi-layered security framework for enhancing the security of information systems. The study developed a cryptographic based algorithm to validate a proof of concept of the developed framework for enhancing the security of information systems.

1.8 Thesis Report Organization

The thesis report was organized into six chapters. Chapter 1 introduces the background to the research problem. Chapter 2 is about the literature review. Chapter 3 is about research methodology. Chapter 4 presents the research findings. Chapter 5 presents a discussion of the results. Lastly, Chapter 6 presents the conclusion and recommendations.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents the literature review related to the research problem and research objectives. The research problem addressed was the failure to ensure security goals (confidentiality, integrity and availability) in IS, case of the education sector in Tanzania. It presents information systems security concepts. It presents a soft systems methodology and design science research concepts. Furthermore, it presents the related work and the research gap in relation to the research problem. Lastly, it presents a conceptual framework as a roadmap to guide the research process.

2.2 Information Systems Security

Information system comprises of a set of components for capturing, storing, and processing data and for delivering information, knowledge, and digital products (Wihitmen & Mattord, 2012). The information exists in different information states in IS. The information states can be categorized into capturing, processing, storage and transmissions in IS. The main concern is how to ensure the security of information in IS during information states(NIST, 2012; Bosworth et al., 2014). Security requirements should be defined in each information states in IS to guarantee required security goals (Tipton & Krause, 2008; Bosworth et al., 2014).

In general, the security of information systems is the quality or state of being secured or to be free from danger(Wihitmen & Mattord, 2012). Security of IS is concerned

with ensuring security goals (confidentiality, integrity and availability) for information in IS (Bosworth et al., 2014). Information systems security (ISS) is the protection of information in IS from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (NIST, 2012). ISS is achieved through implementing technical, management, and operational measures designed to protect confidentiality, integrity and availability of information (Feruza & Kim, 2007; Nachtigal, 2009; Norman & Yasin, 2010; Wihitmen & Mattord, 2012).

All organizations having IS, websites, intranet, and the Internet are subject to a number of constantly increasing security threats. As risk level grows and the need for organizational compliance in this field increases, ISS becomes more important to an organization's overall business approach (Alshboul, 2010; Wihitmen & Mattord, 2012). System security life cycle, like software life development life cycle, it has phases. It is comprised of the ignition phase, development/acquisition phase, implementation phase, operation/maintenance phase and disposal phase of system security cycle.

During system security lifecycle, capturing state such as input validation is always forgotten (OWASP, 2017) in SDLC. Attackers can bypass authentication of IS through parameter modification, session ID prediction, SQL injection and cross-site scripting (Lawal et al., 2016; OWASP, 2017). Systems development life cycle concentrates on functional requirements. Systems security requirements are collected and implemented after the system has been developed and is about to be deployed in the production environment. Before system development starts an adequate system

development life cycle (SDLC) must define security requirements at each stage of SDLC (OWASP, 2017).

The security requirements for information in IS should include security mechanisms for user management, authentication, authorization, data confidentiality, integrity, availability, accountability, session management, transport security, tiered system segregation, and legislative and standard compliances. The traditional approach is to specify technical controls such as SSL/TLS to enhance the security of information during transmission state in IS. It does not follow the systems security life cycle. SSL/TLS can be bypassed, and hackers can access data/information in capturing state, storage states and processing state (Baset & Denning, 2017). The attacks can be through SQL injections, cross-site scripting, invalidated inputs textboxes, heart bleed attacks, cybercrimes, and malicious codes attacks. The system deployed with miss-configuration settings, default settings. Security testing such as penetration and vulnerability testing is not given equal weight as functional requirements. This result in deploying insecure IS which are vulnerable to cyber-attacks (OWASP, 2017). For secure IS, SDLC should incorporate security requirements for ensuring security goals in each phase of SDLC.

2.2.1 Security Goals

The security goals (or security services) includes availability, integrity, authenticity, confidentiality, privacy, and non-repudiation (Krutz & Vines, 2007; NIST, 2012). Many information security professionals (Krutz & Vines, 2007; Tipton & Krause, 2008) have argued that security goals can be mainly grouped into confidentiality,

integrity, and availability (CIA) triad. This grouping depends on how you broaden the CIA triad to include other security goals such as authenticity and non-repudiation (Breithaupt & Merkow, 2014). The study grouped security goals into three categories, namely: confidentiality, integrity, and availability. The other security goals are included in these three categories (Bosworth et al., 2014). The discussion of each of security goals is as follows.

2.2.1.1 Integrity

Integrity is the guarantee that the message sent is the one received and that the message is not intentionally or unintentionally altered (Demesie Yalew et al., 2017). The data integrity ensures that data has not been modified by unauthorized individuals/systems (NIST, 2012; Bosworth et al., 2014; Sun et al., 2019) during information states (capturing, processing, storage and transmission). The changes made to data/information or IS are done only by authorized individuals, systems. Corruption of data is a failure to maintain data integrity (Kruz & Vines, 2007; Tipton & Krause, 2008). Integrity ensures the consistency, accuracy, and trustworthiness of data/information in IS over its lifecycle. Integrity includes ensuring non-repudiation and authenticity of data/information in IS. Nonrepudiation provides guarantees of message transmission between sender and receiver. Authenticity ensuring proof of the origin (Demesie Yalew et al., 2017).

The loss of integrity can occur due to insertion, deletion, omission, use or production of false unacceptable data, modification, replacement, removal, appending, aggregating, separating, or re-ordering, misrepresentation, repudiation (rejecting as

untrue), misuse or failure to use as required (Bosworth et al., 2014). Integrity has three goals. Firstly, to prevent unauthorized users from making modifications to data or programs (Breithaupt & Merkow, 2014). Secondly, to prevent authorized users from making improper or unauthorized modifications (Watkins & Wallace, 2008). Thirdly, to maintain internal and external consistency of data, programs, the information in IS (Bragg et al., 2008; Breithaupt & Merkow, 2014). Integrity attacks result in loss of data integrity, unreliable data, inaccurate data, inconsistency data, and fraud. Thus, much uncertainty still exists about how to ensure the integrity of information in IS in cyberspace across the globe.

The violation of integrity can be caused by various security incidents such as cyber-attacks (Kaspersky, 2017; Symantec, 2017) to information and IS. Some of the integrity attacks include salami attack, data diddling, trust relationship exploitation, password attack, botnet; hijacking a session, man-in-the-middle attack, malicious codes, phishing, misconfigured information systems, SQL injection and cross-site scripting (Watkins & Wallace, 2008; OWASP, 2017; Symantec, 2017). The researchers have been trying to address the loss of integrity of information by employing technical and non-technical solutions. One of the technical techniques employed is cryptographic techniques.

The cryptographic techniques for ensuring the integrity of information in IS includes cryptographic hash, cryptographic message authentication codes, and digital signatures. A hash function is cryptographic one-way function computing fixed length of an input message (Kessler, 2019) to return hash value/hash code or digest (called a digital fingerprint/thumbprint). Hash functions algorithms include Message

Digest (MD) algorithms (Such as MD2, MD4, MD5); Secure Hash Algorithm (SHA) (such as SHA-1, SHA-2, SHA-3). SHA-1 and MD5 are considered as insecure (Bosworth et al., 2014). The requirements properties of hash functions include arbitrary input length; fixed short output length; efficient; one-way function (irreversible output); and collision resistance for hash values.

The application of hash functions for generating hash values can be used for ensuring integrity. They are subject to cyber-attacks such as collision attacks/birthday paradox attacks (Kessler, 2019). Additionally, cyber-criminals can even substitute both the input message and the hash values. Hash values can ensure integrity but cannot ensure non-repudiation and authenticity of the message. Hash functions are used to create a Message Authentication Code (MAC) (also called cryptographic checksum or keyed hash function) and hashed Message Authentication Code (HMAC) (Suhail et al., 2019). MAC involves using a symmetric key to compute authentication tag (tag_{auth}); $tag_{auth} = MAC_k(x) = h(k \parallel x)$ called prefix MAC (Bosworth et al., 2014). The MAC still suffers from hash man-in-the-middle attacks and brute-force attacks (Bosworth et al., 2014); attackers can append a malicious message to the end of the original message x undetected.

HMAC is a hash-based message authentication code (Suhail et al., 2019) on the use of nested secret prefix MACs consisting of inner and outer hash with padding and incrementing key size k ; $tag_{auth} = HMAC_k(x) = h[(k^+ \oplus opad) \parallel h[(k \oplus ipad) \parallel x]]$ (Bosworth et al., 2014). HMAC is mostly used in real practice in ensuring integrity and authentication (Suhail et al., 2019) during transmission like in https protocol. It has

been incorporated in SSL/TLS in web-browsers for securing web-based IS. Both MACs and HMACs provide authentication and integrity of the message/information but they cannot provide non-repudiation because they use symmetric key cryptography with exchanging key k (Kessler, 2019). This risk can only be addressed by using a digital signature.

A digital signature is similar to conventional to the traditional paper signing process. It used for verifying/proving the authenticity of the original digital message/document/data using cryptography techniques (Alizai et al., 2018). First, the user needs to generate private and public key using asymmetric signature algorithms (Aufa et al., 2018) such as RSA, Digital signature algorithm (DSA), and ElGamal Encryption Algorithm. The public key is shared through public key infrastructure with a trusted external certificate authority (CA) like Verisign and DigiCert; included a digital certificate of the key owner. It is created by the computing hash of the original digital message; the hash value (digital fingerprint) is encrypted with a private key of the sender to form a digital signature (Bosworth et al., 2014).

The receiver verifies the signature by using the public key of the sender. The digital signature ensures integrity, authenticity and non-repudiation of the message (Kessler, 2019). The problem remains is how to ensure the authenticity of the public key and strength of the algorithm used; and how do you handle your private key. Non-technical means such as policy, security awareness are required. But the problem of loss of integrity of information in IS due to cyber-attacks such as SQL injections and cross-site scripting is on the rise (Alsmadi & Alazzam, 2016; OWASP, 2017).

2.2.1.2 Confidentiality

Confidentiality is concerned with the prevention of intentional or unintentional unauthorized disclosure or observation of contents (Bosworth et al., 2014; Demesie Yalew et al., 2017). It includes means for the protection of privacy and proprietary information in IS (Onica et al., 2016). Maintaining confidentiality requires that data cannot be observed or disclosed by unauthorized individuals, systems or processes (Beissel, 2014) and thus cannot be compromised. The breaches of confidentiality can occur through disclosing, accessing (locating), observing, monitoring and acquiring, copying of information/data (Bosworth et al., 2014). The violation of confidentiality can result in the unauthorized disclosure of sensitive data and information (NIST, 2012; Demesie Yalew et al., 2017).

Confidentiality attacks result in a violation of privacy, unauthorized access to information, identity theft (Onica et al., 2016). Sensitive information leaks through malicious activities, technical and non-technical means or a combination. Some of the confidentiality attacks approaches are packet capture, ping sweep, and port scan, dumpster diving, electromagnetic interference (EMI) interception, wiretapping, social engineering, sending information over overt channels (Sood & Enbody, 2011; Barker & Morris, 2013; OMNISECU, 2017).

Social engineering is becoming one of the attacks for disclosure of sensitive information. Social engineering attacks involve psychological manipulation of the mindset of people, fooling of users or employees into handing over confidential or sensitive data to an unauthorized person or system (Luo et al., 2011). It is normally accomplished by sending e-mails or SMS (SMiShing) with malicious links to

execute (Luo et al., 2011; Ayyagari & Tyks, 2012). A number of identities stolen; social engineering, malware, spam, & phishing, SMiShing is on the rise(Symantec, 2017). Malicious software has resulted in the breaches of confidentiality of the information in IS (Robert & Hemalatha, 2013).

Breaches of confidentiality is due to phishing attack, identity theft, malicious attacks (such computer viruses, Trojan, worms), leaking of confidential information by insider, security misconfiguration, broken authentication and access control, SQL injection, cross-site scripting, and XPath injection attacks(Barker & Morris, 2013; Kanure et al., 2014; Tayade & Wadhe, 2014; OMNISECU, 2017; OWASP, 2017). Researchers have been trying to address these breaches using technical and non-technical approaches. Some of the techniques approach employed in addressing confidentiality breaches are cryptographic techniques; mainly encryption.

Encryption of information in IS can be achieved through asymmetric encryption or symmetric encryption. Asymmetric encryption (also called public cryptography) use different keys (public key and private key pair) for encryption of plaintext and decryption of ciphertext (Kessler, 2019). Asymmetric algorithms commonly in use in practice includes are RSA (Rivest, Shamir, Adleman) algorithm, El Gamal algorithm and Elliptic Curve Cryptography (ECC)(Hussain et al., 2019). Symmetric encryption (also called secret encryption/cryptography) uses the same key for encryption and decryption of plaintext and ciphertext respectively (Bosworth et al., 2014). One of the symmetric encryption algorithm schemes is 3DES (Triple Data Encryption Standard) and AES (Advanced Encryption Standard).

The symmetric encryption is faster compared to asymmetric algorithms. But the challenge for symmetric is a key exchange between sending and receiving parties. For e-commerce, asymmetric encryption is used to ensure confidentiality of data. For massive encryption of data/information during storage, a hybrid of symmetric (for encryption of data/information) and asymmetric encryption (for exchange of keys) is used(Hussain et al., 2019).

Diffie Hellman cryptographic algorithm is employed for securing cryptographic keys exchange (Kessler, 2019) over an untrusted network such as the Internet. The application of hybrid of asymmetric and symmetric encryption is employed in e-commerce through protocols such as SSL/TLS(Hussain et al., 2019). It is employed in the creation of secure communication channels for extending LAN/INTRANET over an untrusted network such as the Internet using IPsec (site to site VPN or remote access VPN)(Hussain et al., 2019).

Encryption algorithms are subject to crypto attacks such as cryptanalysis brute force attacks, birthday paradox attacks (Bosworth et al., 2014) and social engineering attacks. Thus, encryption alone cannot ensure the confidentiality of information. Cyber-attacks such as SQL injections (OWASP, 2017) and cross-site scripting can by-pass even strong encryption and authentication (Alsmadi & Alazzam, 2016) in IS. Thus, it is due to insecure coding practices; failure of incorporating security requirements in SDLC. Traditional practices of incorporating SSL/TLS during the implementation of IS have not resulted in ensuring the confidentiality of the information in IS during capturing, processing, storage and transmission of

information.

2.2.1.3 Availability

Availability includes elements that create reliability and stability to access information in IS (NIST, 2012; Verma et al., 2014; Chernov & Sychugov, 2019). It is timely, reliable access to information in IS for authorized users (Bhosale et al., 2018). Availability ensures that information in IS are accessible as needed and where needed by authorized users, systems or processes (Chand & Mathivanan, 2016). It guarantees that information in IS are accessible when needed, allowing authorized users to access the IS and other IT resources (Chand & Mathivanan, 2016; Bhosale et al., 2018).

Loss of availability can occur due to destruction, damage or contamination, denial, prolongation or maintenance, acceleration or delay in use or acquisition. Some of the availability attacks includes denial of services (DoS), distributed denial of service (DDoS), TCP SYN flood, Internet Control Message Protocol (ICMP) attacks, electrical disturbances and attacks on system's physical environment (Jerschow, 2012; Vijayasarathy, 2012; Shiaeles, 2013; Rudman, 2014; OWASP, 2017). Attackers like ransomware attacks can make the information in IS unavailable to legitimate users (Bosworth et al., 2014) by hiding it or denying its use through encryption and not revealing the means to restore it. The disruption of access to or use of information or an information system results in the denial of services to legitimate users. The loss of availability of information in IS can lead to business disruption, loss of customer confidence, loss of revenue (Chernov & Sychugov, 2019).

2.2.2 Security of Assets

Security is concerned with the protection of assets (Krutz & Vines, 2007; Mumtaz, 2015) by ensuring security goals (confidentiality, integrity and availability) are guaranteed. An asset includes data, information, information systems, IT infrastructures, devices, databases, hardware (e.g. servers, network devices, etc.), software (mission-critical application, systems and other components of the environment) that support information in IS (Shamala & Ahmad, 2014). Assets can be categorized into information assets, software assets, physical assets and services (computing services outsourced by the organization, communication services: Internet and environmental services such as air conditioning, power)(Mumtaz, 2015). Assets should be protected from unauthorized access, use, disclosure, modification/alteration and damage/destruction(NIST, 2012).

Assets are affected by vulnerabilities, threats and risks associated with. Vulnerabilities are weaknesses, open holes or gaps in a security program that can be exploited by threats to gain unauthorized access, modification/alteration, and damages to a given asset(Bosworth et al., 2014). The threat is anything that can exploit the vulnerability, intentionally or unintentionally to obtain, damage/destroy and/or theft (NIST, 2012; Bosworth et al., 2014) of a given asset (such as confidential information in IS). The goal is to ensure assets are protected from various threats.

The assets should be classified and assigned a security clearance level(Mumtaz, 2015). It involves identification, accountability of assets preparing a schema for information classification (confidentiality level: public, confidential, secret and top-

secret; value; time sensitivity; access rights; and archive/destruction time) and implementing the classification schema (Krutz & Vines, 2007; Mumtaz, 2015). Security of assets depends on effective security measures and controls to avoid the associated exploitation of vulnerabilities by threats. Risks to assets are the potential for loss, damage or destruction of a given asset as a result of a threat exploiting the vulnerability (Bosworth et al., 2014). The risk to assets is the intersection of assets, threats, and vulnerabilities to the given asset. The risks should be assessed for the given asset.

The risk is a function ($\text{Risk} = \text{Asset} + \text{Threat} + \text{Vulnerability}$) of threats exploiting vulnerabilities to damage/destroy a given asset (NIST, 2012; Shamala & Ahmad, 2014). Threats may exist, but if there are no vulnerabilities to a given asset then there is little/no risk. Additionally, a given asset can have a vulnerability, but if there exists no threat to exploit the vulnerability, then there is little/no risk (Mumtaz, 2015). Assessing vulnerabilities and threats are crucial in determining the risk level profile of the assets such as information in IS. The study specifically is concerned with how to enhance security for information in IS during information states (capturing, processing, storage and transmission).

Ensuring the security of IS involves protecting IT assets through implementing required security measures, and security controls (Krutz & Vines, 2007; Bosworth et al., 2014). Security measures and security controls should be implemented to ensure security goals (confidentiality, integrity and availability) of information in IS during information states as per security requirements. These security requirements for protecting IT assets are stipulated in the security policy of the given organization.

An information security policy provides the formal structures for the given organization or sector for ensuring security responsibility and accountability for information in IS (Tipton & Krause, 2008). It establishes procedures and guidelines for protecting information assets. It creates means for assigning access privileges, creates sanctions for breaches of security at any level of the organization, and requires training in the privacy and security practices of an organization (Bosworth et al., 2014). Furthermore, executives and top management must take the lead to promote the security of information in IS as an important cultural for the given organization or sector (Shaaban, 2014). Too often, the top management believes that security of IS is the responsibility of the ICT Department. ICT and security of IS, do not come into this category unless things have gone enormously wrong, and their responses are to wait for ICT people to recover from the incidents (Bakari, 2007; Gelbsteun, 2012; Shaaban, 2014).

2.3 Enhancing Security of Information Systems

There exist various security models, frameworks, standards and best practices related to enhancing the security of IS. However, ensuring the security of information in IS during information states (capturing, processing, storage and transmission) in information systems is debatable. The discussion of each of them is as follows.

2.3.1 Security Models, Frameworks and Standards

2.3.1.1 Security models

Various security models exist for managing the security of IS: NSTISSC security model, access control models (access matrix, Take-Grant Model and the Bell-LaPaduala Model); integrity models (Biba Integrity Model and the Clark-Wilson

Integrity Model), information inflow models (Non-Interference Model and the Chinese Wall Model); and SABSA security model. The discussion of each of security models is as follows.

I. NSTISSC (NSS) security model

National Security Telecommunications and Information Systems Security Committee (NSTISSC) security model provides a graphical representation of the architectural approach widely used in computer and information security. The NSTISSC security model (McCumber Cube) presents ISS in three dimensions cube (NSTISS, 1994; Wihitmen & Mattord, 2012). NSTISSC security model has its drawbacks.

The NSTISSC model covers the three dimensions of information security (information states: transmission, storage, and processing; critical information characteristics: confidentiality, integrity, and availability; security measures: technology, policy, practice). It omits capturing state (Altaf et al., 2016; OWASP, 2017), and it is too general. Moreover, it omits discussion of detailed guidelines and policies that direct the implementation of controls. The missing capturing state and detailed guidelines need to be incorporated in the framework for enhancing the security of IS.

II. Access control models

Access controls models are security models for controlling access to information or IS aiming at ensuring the confidentiality, integrity, and availability of information in

IS (Krutz & Vines, 2007; Qadir & Quadri, 2016). Some of the access control models include Access matrix, Take-Grant Model, and the Bell-LaPaduala Model.

Access matrix: An access matrix is a straightforward approach that provides access rights to subjects for objects. Access rights are means for ensuring the confidentiality, integrity, and availability of IS (Krutz & Vines, 2007). The access matrix model supports discretionary access control because the entries in the matrix are at the discretion of the individual(s) who have the authorization authority over the table (Lampson, 1974; DeLone & McLean, 2003). Using the access control matrix alone cannot guarantee to ensure security (Dong et al., 2018; Tang et al., 2018) during information states (capturing, processing, storage and transmission). The study incorporates access security in security controls in the developed framework for ensuring the security of IS using a multi-layered security approach.

Take-Grant model: Take-Grant model is one of the access control models for enhancing the security of IS. It uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject (Bishop, 1995; Krutz & Vines, 2007; Promyslov, 2017). It has drawbacks. It is a very general model that does not constrain in any way the set of commands that may be used to manipulate rights in IS (Bishop, 1995). This limitation is incorporated during the development of the framework for enhancing the security of IS.

Bell-LaPadula model (BLP): The BLP is one of the access control model designed to be used for enforcing access control in IS. It is concerned with the confidentiality of classified information based on access clearance level. It is characterized by no

read up constraint; and no write-down constraint in controlling access to classified information. It is restricted to the confidentiality of classified information based on access clearance level.

BLP does not address other information security goals (integrity and availability) (Tang et al., 2018). It contains covert channels. These covert channels create a capability to transfer information that is not supposed to be allowed from one level to another (Lampson, 1973). Unauthorized access to information can occur; which compromises the confidentiality and integrity of information in IS. The drawbacks BLP were taken into consideration during the development of a framework for enhancing the security of IS. The advanced BLP (Balamurugan et al., 2015; Tang et al., 2018) was considered during the development of the framework for enhancing the security of IS by incorporating access controls in IS.

III. Integrity Models

The integrity models include the Biba Integrity Model and the Clark-Wilson Integrity Model. The discussion of each of integrity models is as follows.

The Biba integrity model: The Biba Integrity model is an access control model which address the integrity goal of information security(Krutz & Vines, 2007). This model has limitations which include: how to select the right policy to implement in ensuring the integrity of information (Balon & Thabet, 2004). Moreover, it is limited only to integrity goal; other information security goals are not addressed by this model (does not address confidentiality and availability of information). The drawbacks were incorporated during the development of a framework for enhancing the security of IS.

The Clark-Wilson integrity model: This model is one of the access control model developed to address the integrity goal of information security. It incorporates mechanisms to enforce internal and external consistency, separation of duty, and a mandatory integrity policy (Clark & Wilson, 1987). It was developed specifically to address integrity goal; other information security goals (confidentiality, availability) are not addressed in this model. Its limitation was taken into consideration during the development of a framework for enhancing the security of IS.

IV. Information flow models

The information flow models consist of objects, state transitions, and flow policy states. Information flow models are constrained to flow in the directions that are permitted by the security policy in IS (Krutz & Vines, 2007; Schultz, 2012). Among of these models includes Non-Interference model and Chinese wall model. The discussion of each of them is as follows.

Non-Interference Model: This model is related to the information flow model with restrictions on the information flow (Krutz & Vines, 2007; Mikulcak et al., 2018). The low user is not able to learn anything about high user activities but can learn about any high information that was created through means other than the actions of high users. It is limited to the information flow. It suffers from the risk of covert channel attacks in real world environment setting implementation. Its drawbacks have been addressed during the development of a framework for enhancing the security of IS by employing multi-layered security approaches through security measures and security controls layers.

Chinese wall Model: This model prevents information flow that might result in a conflict of interest in an organization representing competing parties (Krutz & Vines, 2007; Lin, 2015). This model prevents compromise of the sensitive data of either or both parties due to weak access controls in the consulting organization (Krutz & Vines, 2007; Schultz, 2012; Lin, 2015). The model does not entirely stop the flow of inside information and prevent insider trading; nor does it always reduce analysts' conflicts of interest (Gorman, 2004). The idea of preventing the flow of conflicting information in IS was incorporated using multi-layered security approaches. The study incorporates security measures and security controls in the framework for enhancing the security of IS.

V. The business model for information security

This model takes a business-oriented approach to manage security in IS within the context of business (Roessing, 2010). It encompasses elements such as culture, processes, human factors, technology and governance. It does not address how to ensure the security goals of IS in holistic system thinking views. It does not fully address how to assess security requirements and integrate them in SDLC in sector specific like the education sector in Tanzania.

VI. COBIT for information security

Control Objectives for Information and related Technology (COBIT) for information security is a set of principles in which an organization can build and test security policies, standards, guidelines, processes, and controls (ISACA, 2012). This model does not adequately address how to assess, identify and incorporated security requirements for ensuring security goals in SDLC.

2.3.2 Security Standards and Best Practices

The research study explores ISO 27000 series standards related to enhancing the security of IS. The ISO 27000 series for information security management system includes ISO/IEC 27001 and ISO/IEC 27002 standards as explained below.

2.3.2.1 ISO/IEC 27001

ISO 27001 is an information security management system standard for ensuring information security goals (confidentiality, integrity, and availability). This involves selecting, implementing and maintaining the right controls based on risk assessment of the given organization (ISO/IEC 27001:2013, 2013). The research study explored ISO/IEC 27001: 2013 which contains 114 controls. The given organization is required to identify and select the right controls based on risk assessment and the acceptable risk level. The requirements set out in ISO 27001 are generic and need customization to fit in the organization needs by selecting the relevant controls to implement. It does not provide guidance on assessing, identifying in integrating security requirements in SDLC in sector specific like the education sector in Tanzania.

2.3.2.2 ISO/IEC 27002

ISO 27002 is information technology practices standard that gives guidelines for the organization in implementing information security management practices including the selection, implementation and management of controls based on the risk assessment (ISO/IEC 27002:2013, 2013). The research study explored ISO 27002:2013.

The ISO 27002:2013 specifies the codes of practices, guidelines and best practices in

implementing the controls for information security management system requirements as defined in ISO 27001:2013. The standards are too general and need customizations to fit in in the given country and sector context such as the education sector in Tanzania. The customization considered in this research study was to assess and identify security controls relevant to IS for ensuring security goals (confidentiality, integrity and availability) of information during capturing, processing, storage and transmission, a case study of education sector in Tanzania. The study considered these security requirements (security measures and security controls) during the development of a framework for enhancing the security of IS.

2.3.3 Security Domains

Various previous studies have urged that ensuring security of information in IS requires employing a multi-layered security approach similar to Open Systems Interconnection model (OSI model) or (Transmission Control Protocol/Internet Protocol) model(TCP/IP model) structure (Carvalho & Marques, 2019; Rizk et al., 2019; Tanovic & Marjanovic, 2019; Uctu et al., 2019). In order to address the research problem of loss of confidentiality, integrity and availability of information in IS; the study used a multi-layered security approach.

The security layers in this study were grouped into 15 security domains(NIST, 2012; ISO/IEC 27001:2013, 2013; ISO/IEC 27002:2013, 2013; Tanovic & Marjanovic, 2019), namely: information security policy, organisational of information security, human resources security, asset management, access control, cryptography, physical and environmental security, operations security, communication security, systems acquisition, development and maintenance, supplier relationships, information

security incident management, information security aspects of business continuity management, compliance, and risk management. Security requirements (in terms of security measures and security controls) for ensuring security goals (confidentiality, integrity and availability) of information in IS were assessed and defined in each security domain (Rizk et al., 2019; Tanovic & Marjanovic, 2019). Security domains were incorporated during the development of a multi-layered security framework for enhancing the security of information systems, a case study of the education sector in Tanzania. It was guided by a Soft Systems methodology (Checkland, 1998) and design science research (Hevner et al., 2004; Gregor & Hevner, 2013).

2.4 Soft Systems Methodology and Design Science Research

The study adopted a soft systems methodology compounded with design science research to guide the research process. The explanations are as follows.

2.4.1 Soft Systems Methodology

The study has adopted a soft systems methodology compounded with DSR to guide the research process (Section 3.2). Soft system methodology (SSM) is the methodology which assists people in solving complex ill-defined problematic situations in the organization (Checkland, 1998; Sensuse & Ramadhan, 2012). The ill-defined problematic situation involving the human factor in this study is a failure to ensure the security of information systems. SSM uses systems rules and principles that allow structuring the system thinking about the real world (Smyth & Checkland, 1976; Checkland & Scholes, 1990; Novani *et al.*, 2014). The study employed employ SSM in conjunction with DSR as the weaknesses of one is complemented by the strengths of the other.

2.4.2 Design Science Research

Design science research (DSR) is the research methodology used for creation and evaluation of IS artifacts (Peppers et al., 2012; Razali, 2018) intended to solve an identified organizational problematic situation such as failure to ensure the security of information systems (Section 3.2.2). DSR involves the design and creation of information technology artifacts. These are constructs (vocabulary and symbols), models, methods, algorithms, and instantiations (Hevner et al., 2004). In this study, the desired artifact was the development of a framework for enhancing the security of information systems. DSR compounded with SSM was adopted to guide the research process.

2.5 Related Work

Various studies have proposed solutions to address the problem of loss of security goals (confidentiality, integrity and availability) for information in IS. A study by Chaula (2006) proposed a framework for security assurance by incorporating security requirements to improve the security of IS using the social-technical approach, a case study of TANESCO. Chaula's study examined culture, usability problems, and security internal controls. Chaula's framework was based on re-use of security requirements of TANESCO information system which may not fit in other sectors like education sector in Tanzania. The research study addressed these limitations by developing a framework for enhancing the security of IS by incorporating security measures and security controls.

A study by Bakari (2007) proposed a framework for managing ICT security in non-commercial organisations. Bakari identified 12 components and one of them is

developing countermeasures. The author argues that for developing security countermeasures, you are required to use best practices such as ITIL, ISO 177799 and COBIT; these are generic global standards which customization by itself is a challenge. Bakari's framework suffers from inadequate incorporations of security measures and security controls for ensuring the security of IS. The research study addresses these limitations by unfolding those generic standards and incorporating them in the developed framework in terms of security measures and security controls components using a multi-layered security approach.

A study by Chatfield (2009) developed a framework intelligent environments for addressing privacy and security. Chatfield's framework was limited to privacy and security requirements of intelligent environments. The study addressed these limitations by incorporating security measures and security controls during the development of a framework for enhancing the security of IS. A study by Ismail et al. (2010) proposed a framework for managing information security for Malaysian academic environment; by identifying 5 elements. This framework suffers from the narrow scope of a framework for managing the security of IS. Additionally, the security culture of Malaysian can be different from that of the education sector in Tanzania. These limitations were addressed in this research study by developing a framework for enhancing the security of IS in Tanzania, the case of the education sector.

Alfawaz (2011) developed a framework for information security culture in the context of Saudi Arabia (developing country). Alfawaz's framework is limited to security culture in Saudi Arabia which may not fit in Tanzania context such as the

education sector. The research study addresses these drawbacks, by developing a framework for enhancing the security of IS. A study by Awad & Battah (2011) proposed a two-tier model for enhancing the security of information system in educational organizations.

The proposed model is limited to policy and laws of the information system; and a technical approach on how to audit the security of the information system. Kapis (2011) addressed the problem of failure to ensure security in IS by addressing security and privacy in IS, but the context was limited to the case of the hospital. The research study addresses these drawback by developing a framework for enhancing the security of IS, a case study of the Education sector in Tanzania.

A study by Karokola (2012) proposed a framework that would facilitate Government organizations to effectively offer appropriate secure e-Government services (using six organizations). Karokola developed framework targeted on integrating security services to thee-Government Maturity Model (e-GMM). Karokola proposed solution was limited to securing e-GMM; it's more a maturity evaluation model for e-government adoption and implementation of e-services. Karokola argued that security requirements should be incorporated in the framework to ensure security goals (CIA triad) for information during capturing, processing, storage and transmission in IS. Karokola study was limited to the adoption and usage of e-services in Tanzania. Karokola did not adequately incorporate security requirements during SDLC. These limitations were addressed in this study by incorporating

security requirements (security measures and security controls) in the developed framework for enhancing the security of information systems.

Kasita & Laizer (2013) developed security architecture for Data-warehouse for the higher learning institutions in Tanzania. It is limited to security requirements for the data warehouse. Moreover, a study by Shaaban (2014) proposed a framework for improving security based on governance information security culture. Shaaban's proposed identified security requirements which were limited to the context of Zanzibar public based on information security culture. These limitations were addressed by incorporating security measures and security controls in the developed framework for enhancing the security of information systems.

A study by Mbowe et al. (2016) proposed a framework for threat assessments in IS based on Microsoft advanced analytics model (Microsoft, 2002) (STRIDE threat model). It integrates information security policy into a developed framework for threat assessment. It is a vendor-based model which implies that extension to other environments such as the education sector in Tanzania, does not guarantee to give desired results. These limitations were incorporated in the developed framework for enhancing the security of information systems; by fusing those identified security requirements in the security domain (assessment of security compliance) layer.

2.5.1 Security Measures for Ensuring Security Goals

The research study reviewed related literature in relation to security measures for ensuring security goals (confidentiality, integrity and availability) of information in IS. These security measures address security goals (CIA triad). The security goals

involve protecting the confidentiality of information, preserving the integrity of information and promoting the availability of information in IS for authorized use (Breithaupt & Merkow, 2014).

2.5.1.1 Confidentiality

Breach of confidentiality of the information in IS during information states is a problematic situation researchers are trying to address. Different studies have tried to come out with solutions to prevent intentional or unintentional unauthorized disclosure or observation of data. Loss of confidentiality is always difficult to be detected or tracked as information or data can be viewed/read or copied without leaving any track back or footprint to track upon (Bosworth et al., 2014).

A study by Robert & Hemalatha(2013) proposed efficient malware detection and tracer. According to Beissel (2014), the use of antimalware such antivirus can mitigate some attacks resulted from malware. However, sophisticated attacks such Heartbleed attacks (MITRE, 2014) can result to stolen or leakages of secret information such as secret keys, passwords, and personally identifiable information (such as credit card numbers) during the processing of information in the memory of servers.

The attackers employ different techniques to get confidential data/information. Massive leaks of confidential information happened in the scandals of Edward Snowden and WikiLeaks scandals (REUTERS, 2014). The loss of confidentiality is the results of the failure of authentication and session management in IS. Research findings from OWASP (2017) revealed that authentication and session management

in IS are often implemented incorrectly, allowing attackers to compromise the user's identity or session tokens.

The loss of confidentiality is the result of misconfigured IS (Shamsi & Khojaye, 2018). The misconfigured IS are vulnerable to injection flaws such as SQL injection, cross-site scripting, E-mail (IMAP/ SMTP) injection and other attacks (OWASP, 2017). A study by Lubis et al. (2018) pointed out that a confidentiality breach is the result of security misconfiguration of IS. These attacks can bypass authentication and authorization. The attacks can cause spam relay, spam (for the case of IMAP/SMTP) injection attacks and information leakages. Likewise, XPath injection attacks execute crafted XPath queries into the application to gain access to unauthorized data and bypass authentication. It is commonly a result of insecure default configurations, incomplete or ad hoc configurations for IS during information states.

Restrictions on what authenticated users are allowed to do are often not properly enforced in IS (Liu & Kavakli, 2018). This causes information disclosure to unauthorized individuals/systems. Thus, it results in a loss of confidentiality of the information in IS. The confidentiality of the information in IS depends on effective security measures, and their correct settings and configuration to safeguard information in IS during information states (capturing, processing, storage and transmission).

Ensuring the confidentiality of the information in IS could entail physically or logically restricting access to sensitive data or encrypting sensitive data traffic

traversing a network(NIST, 2012; Bosworth et al., 2014). Studies by Cleeff (2015) and Talib (2015) pointed out that only authorized individuals and systems are required to view (or access) sensitive or classified information. This also implies that unauthorized individuals should not have any type of access (Talib, 2015) to the data or IS. The individuals or systems should be identified and authenticated based on information sensitivity classification and security clearance level (Cleeff, 2015; Talib, 2015). A study by Varshney et al. (2018) proposed identification and authentication security measures for addressing breaches of confidentiality of the information in IS. But it was limited to Bluetooth devices authentication mechanisms. It did not fully address security measures for ensuring the confidentiality of information during information states (capturing, processing, storage and transmission) in IS.

Joshi et al. (2017) pointed out that confidentiality of the information in IS can be enhanced using attributed based access control organization confidentiality policy. It was limited to Bell LaPadula model confidentiality policy; limiting to systems environments which security levels do not change dynamically. According to studies by Nabeel (2017) and Sultan et al. (2018)pointed out that confidentiality of information can be ensured through end to end encryption at the physical layer. But IS secured via end to end encryption are broken down due to flawed design of IS and security assumptions business logic (OWASP, 2017). A study by Agrawal et al. (2018) argued that for enhancing confidentiality logs of sensitive data should be monitored and secured. Furthermore, security awareness (Kolli et al., 2018) should be conducted to users and stakeholders of IS. The awareness should include

identification and implementation of effective security measures for ensuring the confidentiality of the information in IS during information states (capturing, processing, storage and transmission) in IS.

The users of IS and ICT devices creates a huge amount of sensitive data which should be sanitized during capturing or destroyed when reaches its end of lifespan(Fundo et al., 2014; Kissel & Scholl, 2014; Tambe & Vora, 2016; Aissaoui et al., 2017). A study by Tambe & Vora (2016) argued that sensitive data collected should be sanitized after use. It proposed a system for accepting inputs and producing sanitized outputs. Likewise, a study by Aissaoui et al. (2017) pointed out that residual data generated by IS should be sanitized. The sanitization of sensitive data during information states has not fully been addressed. Thus, ensuring the confidentiality of the information in IS during information states (capturing, processing, storage and transmission) in IS is debatable. Security measures for ensuring the confidentiality of the information in IS should be identified and implemented during information states in IS.

Security measures for ensuring the confidentiality of the information in IS includes segmentation of the network (using firewall rules, VLAN), identification and authentication (Beissel, 2014; Varshney et al., 2018). Additionally, the confidentiality of information can be guaranteed using authorisation, access controls, encryption of internal data transmission (using encryption software, SSH, VPN, SSL/TLS), encryption of external data transmission and encryption of files and encryption of hard drives (Nabeel, 2017; Sultan et al., 2018).

Furthermore, it can be guaranteed through secure deletion of files, destroying or degaussing physical media, protection against vulnerabilities, use of antivirus software, security awareness and training; and logging, monitoring and alerting (using log management), IDS, IPS(Beissel, 2014; Kissel & Scholl, 2014; Tambe & Vora, 2016; Aissaoui et al., 2017; Agrawal et al., 2018). The persistence approach of just using CIA triad is inadequate to protect IS hosted in cyberspace from loss of availability. There is a need for comprehensive a multi-layered security framework that assess, identify and integrate appropriate effective security controls and security measures for preserving or minimizing the loss of availability of IS in practical terms. This study addresses the current limitations of the existing solutions which mainly focuses on technologies approaches; omitting the human factor which is the weakest link in security.

2.5.1.2 Integrity

Violation of the integrity of data/information in IS has been a growing challenge for which many researchers are trying to address. Altaf et al. (2016) pointed out that weak validation of text-based input data and unpatched IS are the causes of SQL injection and cross-site scripting. Hackers can exploit these vulnerabilities. Hackers can bypass authentications and authorization to gain administrative (or root) access to databases and IS infrastructure. This can lead to integrity violation of data and IS. A study by Mirza (2016) argued that information can change even one bit or more while traversing through the network. This leads to loss of integrity of information. The existence of sophisticated tools designed to assist network and systems administrators to monitor, analyze networks and systems to mitigate cyber-attacks

are now becoming a weapon for cybercriminals(Altaf et al., 2016).

Studies by Alsmadi & Alazzam (2016) and Baset & Denning (2017) revealed that many IS are developed without proper input validations. They allow insertion of invalidated data inputs into the given system. Attackers can inject cross-site scripts and SQL injection into IS to gain access through bypassing authentication and authorization. This leads to integrity violation of data in IS. The misconfiguration in IS and input validation failures (or input sanitization failures) are the most causes of injection flaws (SQL injection and cross-site scripting) attacks (OWASP, 2017). These injection flaws cause a violation of the integrity of data/information in IS.

The misconfiguration includes deploying IS with default configurations such as unpatched applications, operating systems, databases, not changing default keys, passwords in devices, databases, applications; and revealing error handling the information to attackers (Alhanahnah & Yan, 2018). Attackers are employing scanning tools to scan and sniff misconfigured IS. Among these tools are systems scanners for packet sniffing tools such as tcpdump, Nmap, Wireshark, OWASP Zed Attack Proxy (ZAP) and Acunetix (Goyal & Goyal, 2017).

The attackers exploit the identified vulnerabilities in the misconfigured IS. A study by Alhanahnah and Yan (2018) found out that improper configuration of IS; causes integrity violation for information in IS. It showed that 71% of the code snippets contain insecure SSL/TLS patterns. The communication between the two parties is subject to various attacks such as eavesdropping and session hijacking attacks. Radivilova et al. (2018) presented a mechanism for intercepting and decrypting

misconfigured SSL/TLS in IS. It employed scanning and sniffing tools such as Wireshark and Acunetix tools. For ensuring the integrity of information security measures should be identified and effectively implemented during information states.

A study by Hermawan & Wardhani (2017) pointed out that the correct implementation of the digital signature can ensure that data has not been altered by unauthorized users. Rezaeighaleh et al. (2018) proposed a time based digital signature for addressing data alteration attacks. The digital signature guarantees that the message is coming from the sender and has not been altered during information states. A study Elkamchouchi (2018) proposed hybrid techniques for digital signature. The challenge is on the strength of an algorithm employed the digital signature. It depends on the trust of the digital signature.

The digital signature should be used in combination with hash checksum. Sharma (2016) proposed cryptography by reverse and checksum implementation to ensure the message has not been altered during information states in IS. A study by Golaghazadeh et al. (2018) proposed a checksum technique to ensure the integrity of the message during transmission in IS. Thus, security measures for ensuring the integrity of information in IS should be effectively identified and implemented.

The security measures for ensuring the integrity of information includes access control, quality assurance, digital signature and checksum (cryptographic hash function, message authentication code). Additionally, it can be guaranteed through rotation of duties, separation of duties, least privilege principle and need to know to

principle. Furthermore, integrity can be ensured through change management for IS; and logging, monitoring and alerting (Gligoroski et al., 2013; Beissel, 2014; Anand & Ryoo, 2017; OMNISECU, 2017). These security measures aim at preserving or minimizing the loss of integrity of information in IS. The existing solutions for implementing security measures for ensuring the integrity of information in IS are inadequate. It lacks a comprehensive multi-layered security framework for assessing, identifying and integrating appropriate security measures for ensuring loss of integrity.

2.5.1.3 Availability

Violation of the availability of information in IS has been a long yet standing problem which has not fully addressed. The loss of availability of information in IS can lead to business disruption, loss of customer confidence, loss of revenue (Bosworth et al., 2014; Breithaupt & Merkow, 2014). Information in IS can be unavailable due to malicious codes (such as viruses, worms, trojans, ransomware attacks) and equipment failures during normal use (Breithaupt & Merkow, 2014).

The loss of availability of IS is caused by natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes) (Rudman, 2014) or misconfiguration of IS, capacity resources limit or outages (Bosworth et al., 2014). Mail systems which are sending spams are automatically blacklisted by mail spam blockers (Khan et al., 2015) such as spamhaus for sending and receiving e-mails from legitimate domains. Injection attack like e-mail (IMAP/SMTP) injection attack can cause spam relay and botnets (Khan et al., 2015) for distributing spam e-mails.

This can cause a mail system being unavailable to legitimate users. These attacks can cause a denial of services (DoS/DDoS) to legitimate users.

A study by Chen & Chen (2017) pointed out that DoS/DDoS is the most causes of violation of the availability of information in IS. DoS/DDoS can be caused by injection attacks. These injection attacks can compromise the operation and availability of IS. Injections attacks such as SQL injection, cross-site scripting can bypass authentication and authorization(OWASP, 2017). This compromises the whole information system. It causes a loss of availability of information in IS. Thus, ensuring the availability of information in IS during information states (capturing, processing, storage and transmission) is questionable. For ensuring the availability of information in IS, there is a need to define, configure and implement effective security measures in each information states to address the challenges to availability.

The loss availability should be preserved or minimized using technical and non-technical controls. These include capacity planning, sufficient capacity and fault tolerance (Mahimane, 2013; Lane, 2014). Availability of information in IS is ensured through effective backups and testing restores. For ensuring the availability of IS, an organization should have a business continuity plan, system monitoring, and incident management and response (Alhazmi, 2015; Kaczmarczyk, 2015). Capacity planning involves determining the threshold such as bandwidth requirements, performance and resilience requirements (Mahimane, 2013) for IS. Availability of IS can be guaranteed by hardware and infrastructure that are ready for use and have sufficient capacity to process all requests as quickly as necessary (Baruah, 2013). An attacker can compromise the information system with requests

and, thus, cause a denial of service (Qadir & Quadri, 2016).

Availability is guaranteed by scheduled proactive maintenance and emergency maintenance of IS components such performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts (Sabena, 2015). Furthermore, it can be guaranteed by providing adequate communication bandwidth and preventing the occurrence of bottlenecks (Line, 2015). Another availability measures include redundancy, failover, RAID (redundant array of independent disks) and high-availability clusters for mitigating serious consequences when hardware failures happen (Qadir & Quadri, 2016).

The availability countermeasures against data loss or network infrastructure failure must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup should be tested and stored in a geographically-isolated location with fireproof and waterproof safe (Beissel, 2014). These safeguards aim at preserving or minimizing the loss of availability of IS. The existing solutions for implementing security measures for ensuring the availability of information in IS are inadequate. It lacks a comprehensive multi-layered security framework for assessing, identifying and integrating appropriate security measures for ensuring loss of availability.

2.5.2 Security Controls

Security controls are defined and applied based on data classification, security levels and security clearance level (Balliu, 2014; Guelcher, 2015; Alkhudhayr et al., 2019).

Although no single standard exists for data classification, organizations often benefit from examining classification models commonly used by Government (data security label includes unclassified, sensitive but unclassified, confidential, secret and top secret) and many businesses (data security label includes public, sensitive, private and confidential) (Guernic, 2007; Guelcher, 2015; Alkudhayr et al., 2019). Each organization's information resources must be evaluated to determine their information security requirements (Alshboul, 2010; Balliu, 2014; Koo et al., 2019).

Security of information in IS hosted in cyberspace is quite poor due to developers do not use secure coding best practices (OWASP, 2017). The traditional, focus is on the implementation of functional requirements to meet user's requirements and neglect security requirements (Purcell, 2015). A study by Navarro-Machuca & Chen, (2016) pointed out that security in software applications is frequently not taken into consideration during software applications development. Developers give little attention to how to implement security controls during the system development life cycle. This practice introduces vulnerabilities, in which hackers frequently exploit them.

The threat to information in IS can originate from the inside (inside attackers) or outside (outside attackers). Physical isolation of the network for IS do not ensure security to information in IS (Farag et al., 2014; Alkudhayr et al., 2019). It is practical rarely feasible in providing e-services. Connecting IS to external networks such as through the Internet increases cyber-attacks. Security incidents (threat attacks) originate from insider attackers (Kaspersky, 2017; Sviridov et al., 2019). A

study by Addy & Bala (2016) proposed physical access control solution based on biometric authentication techniques with multi-factor authentication. Its design included a multifactor authentication using username and password, facial recognition and fingerprint technology. But, it was limited to a GSM network.

A study by Zhe et al. (2017) proposed a data security policy for enhancing security in cloud storage. It was limited in terms of applicability to cloud storage context. According to Gomes et al. (2017), the business continuity plan should include a technological and organizational scientific validated solution. It proposed enterprise architecture for assisting business continuity planning in the large public organization. This in practice cannot work alone unless combined with other security controls. A study by Fernando (2018) argued that for ensuring the availability of IS in case of disaster, organizations should have effective IT disaster recovery plan to ensure continuity of business in the given organization. For ensuring the security of IS, organizations should employ a combination of effective security controls during information states (capturing, processing, storage and transmission) in IS.

Security controls can be categorized as administrative controls, physical controls, technical controls and compliance controls (Gangire et al., 2019). The security controls should be effectively implemented based on security requirements (Sviridov et al., 2019). According to Watkins & Wallacen (2008) applying technical controls only will not ensure the security of information in IS. Most attacks originating from inside are not technical attacks, non-technical mitigation strategies are required to mitigate them. For ensuring the security of information in IS; a multi-layered security approach should be employed (Rizk et al., 2019; Uctu et al., 2019). It should

integrate all categories of security controls based on security requirements (Koo et al., 2019) for information in IS during information states (capturing, processing, storage and transmission). The discussion of each of security controls is as follows.

Administrative controls are primarily based on policy(Watkins & Wallace, 2008; Kitindi et al., 2014). Administrative controls include routine security awareness training programs; security policies; a change management system, which notifies appropriate parties of system changes; logging configuration changes; properly screening potential employees (for example vetting, performing criminal background checks) (Bosworth et al., 2014; Drago, 2015; Carvalho & Marques, 2019; Toapanta et al., 2019). Security policies describe how information should be restricted and what social changes, procedures, and technologies are required to enforce these restrictions (Shaaban, 2014; Alotaibi et al., 2016; Gangire et al., 2019). A security policy should clearly and concisely express what the protection methods are to achieve, the current threats to security and how these threats should be overcome (Ismail et al., 2010; Awad & Battah, 2011; Drago, 2015; Jones et al., 2017; Carvalho & Marques, 2019).

A study by Alotaibi et al. (2016) pointed out that non-compliance with information security policy is one of the major challenges facing organizations. This is primarily considered as a human problem (Soltanmohammadi et al., 2013; Gangire et al., 2019) rather than a technical issue. Thus, it is not surprising that employees are one of the major underlying causes of breaches (Abelson et al., 2015; Alotaibi et al., 2016; Gangire et al., 2019) in IS security. Thus, in order to ensure the security of IS organization should implement effective, efficacy and efficient administrative

controls through effective design and implementation of information security policy to protect IT resources.

Moreover, physical controls should be given special attention in order to mitigate security threats which can affect IS through physical environments. Physical controls help protect the data's environment and prevent potential attackers from readily having physical access to the data (Shaaban, 2014; Drago, 2015; Jillepalli et al., 2017). These include security system to monitor for intruders (CCTV), physical security barriers (for example, locked doors), climate protection system to maintain proper temperature and humidity. Despite having alerting personnel in the event of a fire, security personnel should guard the data (Alotaibi et al., 2016; PCI-DSS, 2016; Jillepalli et al., 2017; Jones et al., 2017). Other controls such as effective technical controls should be implemented in conjunction with physical controls.

Technical security controls refer to the restriction of access to information resources (Bosworth et al., 2014; Alotaibi et al., 2016). Technical security controls consist of hardware and software features (Shaaban, 2014; Drago, 2015) that help to ensure the security of information by counteracting threats which can impact the IS. Technical controls primarily enforce security requirements (Koo et al., 2019) defined in the security policy (Carvalho & Marques, 2019). Technical controls use a variety of hardware and software technologies to protect data. These include security appliances (for example, firewalls, IPSs, and VPN termination device), authorization applications (for example, RADIUS or TACACS servers, one-time passwords (OTP), and biometric security scanners).

Various studies (Drago, 2015; Symantec, 2016; Ekstedt et al., 2017; Jones et al.,

2017) have shown that the loss of security goal (CIA triad) of information during capturing, processing, storage and transmission in IS are caused by lack or ineffective technical controls (such as misconfiguration of systems, firewalls, the logic error of IS). Thus, there is a need to conduct research on how to enhance IS security by employing security technical controls in conjunction with other security layers such as legal and regulatory or compliance controls.

Legal and regulatory or compliance controls are the countermeasures for enhancing the security of information through conformance with information security policies, standards, laws, and regulations. Compliance controls deal with the management of risks due to the failure to meet the obligations defined in the laws, regulations, policies and contractual agreements (Terblanché, 2013; Weerathunga & Cioraca, 2016). Regulatory compliance is adherence to relevant laws, regulations, guidelines and specifications requirements. Its violations often result in legal punishment, including fines and penalties (Alshboul, 2010; Shaaban, 2014; Alotaibi et al., 2016; Jillepalli et al., 2017).

These security controls (administrative controls, physical controls, technical controls and compliance controls) can further be classified as preventive controls, deterrent controls, detective controls and corrective controls (Watkins & Wallace, 2008). Security controls are weighted by whether they are deterrent, detective preventative or corrective controls (Bosworth et al., 2014). The explanation of each of these controls is as follows.

Deterrent controls are the controls which attempt to prevent a security incident by

influencing (discouraging) the potential attackers not to launch an attack (Huang, 2015; Burton & Straub, 2019). A deterrent control is anything intended to warn an attacker that they should not attack (Otero, 2014). People are less likely to commit security violations acts when they perceive that there will be greater severity, and celerity of sanction against the acts (Otero, 2014; Drago, 2015).

Deterrent controls can include notices of monitoring and logging as well as the visible practice of sound information security management (Straub, 2019). This could be a posted warning notice that they will be prosecuted to the fullest extent of the law. Likewise, deterrent controls such as locks on doors, barricades, lighting, or anything that can delay or discourage an attacker in committing security violations (Huang, 2015; Burton & Straub, 2019). Another IT security control is a detective control.

Detective controls are those controls which can detect when access to data or system occurs (Watkins & Wallace, 2008). Detective controls are in place to detect security violations and alert the defenders by providing earlier warnings. Detective controls include cryptographic checksums, file integrity checkers, antivirus software, system monitoring, intrusion detection system (IDS), motion detector, honeypot, audit trails and logs, and similar mechanisms (Tsegaye & Flowerday, 2014).

Detective controls involve logging of events and the associated monitoring and alerting that facilitate ensuring effective ISS by providing earlier warning alarming (Tsegaye & Flowerday, 2014). Detective controls are the least effective form of controls, but the most frequently used. Detective controls involve identifying events

after they have happened or about to happen (Bragg et al., 2008; Watkins & Wallace, 2008; Tsegaye & Flowerday, 2014). Depending on how quickly the organization can act after the event has been detected; the organization can avoid or limit the magnitude of damages(Bosworth et al., 2014; Huang, 2015).

Preventive controls are the safeguards which attempt to prevent access to data or a system(Bragg et al., 2008; Bosworth et al., 2014). Preventive controls are the safeguards that stop security violations by enforcing access control. Like other controls, preventive controls may be physical, administrative, technical, compliance. Preventive controls can include policies, firewall, antivirus, penetration testing, security awareness training, security guard, intrusion prevention system (Watkins & Wallace, 2008; Tsegaye & Flowerday, 2014). Preventive controls prevent the loss or harm from occurring(Tipton & Krause, 2008; Tsegaye & Flowerday, 2014). Another Security controls are corrective controls.

Corrective controls are the one intended to limit the extent of any damage caused by the incident by recovering the business operations, data and IS to normal working status as efficiently as possible (Bosworth et al., 2014). Corrective controls are one which tries to correct the situation after a security violation has happened. Although after the occurrence of a security violation, not all is lost; it makes sense to try to fix the situation back to normal.

Corrective controls are the ones that minimize the impact of the loss by restoring the system to the point before the event(Watkins & Wallace, 2008). However, the restoration process may result in some degree of loss; may lead to the unavailability

of IS; along with possible lost productivity and customer dissatisfaction (Bosworth et al., 2014; Tsegaye & Flowerday, 2014). For ensuring the security of information, a given organization should implement effective, efficacy and efficient IT security controls based on the security requirements for ensuring security goals (confidentiality, integrity, and availability).

Various studies have revealed that security controls are ineffective (Karakola, 2012; Shaaban, 2014; Drago, 2015; Onica et al., 2016; Jones et al., 2017). For example, a study by Karakola (2012) revealed that security services for securing e-government services are implemented in an ad-hoc manner due to ineffective security controls. This implies that security of IS will be questionable if security controls are not effectively implemented during information states (capturing, processing, storage and transmission) in IS. Furthermore, the literature review revealed that there are inadequate mechanisms for identifying and implementing effective security controls for ensuring security goals (CIA triad) of information in IS during information states (capturing, processing, storage and transmission) in IS.

2.6 Research Gap

There have been a number of valuable studies related to enhancing the security of IS (Bakari, 2007; Kasita & Laizer, 2013; Shaaban, 2014; Mbowe et al., 2016). But there are inadequate assessment and integration of the security measures and security controls in a multi-layered security framework for enhancing the security of information systems (Lawal et al., 2016; OWASP, 2017). The proposed solutions did not adequately incorporate security requirements (security measures and security

controls) during SDLC. Hackers can bypass authentication and authorization to IS using a combination of social engineering and injections attacks such as SQL injection and cross-site scripting (Altaf et al., 2016; Goyal & Goyal, 2017). This results in loss of confidentiality, integrity and availability of information in IS.

The mechanisms for assessing, identifying, implementing and integrating security requirements (security measures and security controls) during SDLC with correct setting and configurations not been fully addressed. The security of information in IS is taken as an afterthought(Unuakhalu et al., 2014) during the SDLC. The existing security models, theories, standards, frameworks(LaPadula & Bell, 1996; Microsoft, 2002; Balon & Thabet, 2004; ISACA, 2009, 2012; Sherwood et al., 2009; ISO/IEC 27001:2013, 2013)are inadequate for ensuring the security of information in IS. Most of them are generic in nature, no guideline specific for customizing them to fit in a context like the education sector in Tanzania.

Correct design, implementation and integration of security measures and security controls to form multi-layered security has not been fully addressed. Ensuring the security of information in IS has been a major concern for more than 45 years(LaPadula & Bell, 1996; Microsoft, 2002; Balon & Thabet, 2004; ISACA, 2009, 2012; Sherwood et al., 2009; ISO/IEC 27001:2013, 2013). The existing models and frameworks are inadequate for ensuring the security of information in IS. They lack a comprehensive security mechanism for accessing, identifying and integrating security requirements (security measures and security controls) in a multi-layered security framework for ensuring security goals of information in IS.

There exist knowledge gap in the application of holistic soft design science systems thinking (SSM and DSR) to the complex problematic situation involving human factor (Checkland, 1998; Salner & Ph, 1999; Hevner et al., 2004; Sanga, 2010) such as enhancing security of IS, case of education sector in Tanzania. This study extends its applications to the enhancement of security of IS by incorporating security requirements (security measures and security controls) during SDLC. The research study addresses the key issues and methodological concern when assessing, identifying and implementing security measures and security controls for enhancing the security of information in IS. These security requirements were incorporated during the development of the framework for enhancing the security of information systems.

2.7 Conceptual Framework

The study proposed a conceptual framework to guide the research process. A conceptual framework was based on concepts from various theories and findings (Green, 2014; Nilsen, 2015) to guide the research. The development of the conceptual framework was guided by SSM integrated with DSR (Checkland, 1998; Hevner & Chatterjee, 2012) in a systematic circular fashion. The conceptual world was compared with the real world to find out feasible desirable change and taking actions to improve the problematic situation (Checkland & Scholes, 1990). The problematic situation in this study was a loss of security goal (confidentiality, integrity and availability) for information in IS during information states in IS, a case of the education sector in Tanzania.

A conceptual framework was used as a blueprint/roadmap for achieving the main research objective. It comprised of a system of concepts, assumptions, expectations, beliefs, and theories that support and informs about the research. It was a key part of the research design (Nachtigal, 2009; Green, 2014; Nilsen, 2015). Figure 2.1 depicts the proposed conceptual framework for enhancing the security of IS in the education sector in Tanzania. It was developed from a literature review, theories concepts, and experience in the research area. The proposed conceptual framework (Figure 2.1) portrays a comprehensive picture of the subject in a systematic way and how was used to address the research problem and research objective.

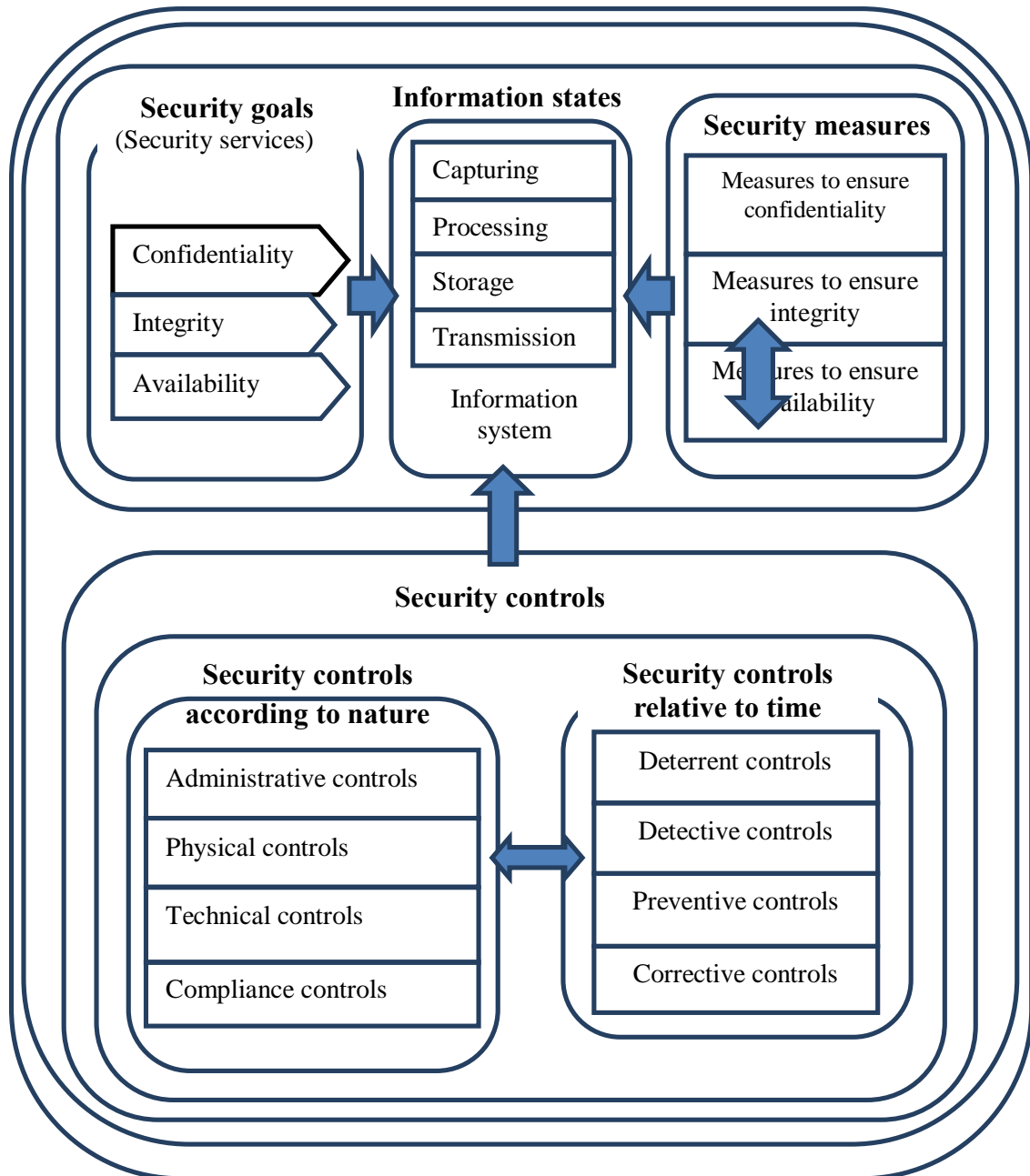


Figure 2.1: Conceptual Framework for Enhancing Security of Information Systems

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter is about the research methodology employed in addressing the research problem. It presents the research paradigms adopted, the research methods employed. It presents the problem of relevance and root definition. Furthermore, it discusses the research design (study area, the sampling design, data collection techniques). It presents access and research ethics. Lastly, it discusses data analysis, validity and reliability of data.

3.2 Research Paradigms

A research paradigm establishes a set of practices that can range from thought patterns to action (Cundill et al., 2012; Mkansi & Acheampong, 2012). In tackling the research problem, the study adopted a soft system methodology compounded with the design science research paradigm.

3.2.1 Soft System Methodology

Soft systems methodology (SSM) is a system thinking approach for tackling real-world ill-defined complex problematic situations in a systematic circular fashion (Checkland & Scholes, 1990). SSM is based on soft systems thinking which focuses on the feedback on the relationships and interactions of the things being studied (Sense & Ramadhan, 2012). It assists people in solving a complex, messy problem in the organization by using systems rules and principles that allow structuring the systems thinking (Checkland, 1998; Novani et al., 2014) about the real world.

The complex problematic situation in this study was the loss of security goals (confidentiality, integrity and availability) for information in IS during information states (capturing, processing, storage, and transmission) in IS. At the heart of SSM, is a comparison between the world as it is, and some models of the world as it might be (Novani et al., 2014). Out of this comparison arise a better understanding of the world (conduct research) and some ideas for improvement (take action) (Checkland & Scholes, 1990; Novani et al., 2014). The SSM has seven stages; some of them address the real world, and some of them perhaps the most important parts address a conceptual world (Figure 3.1).

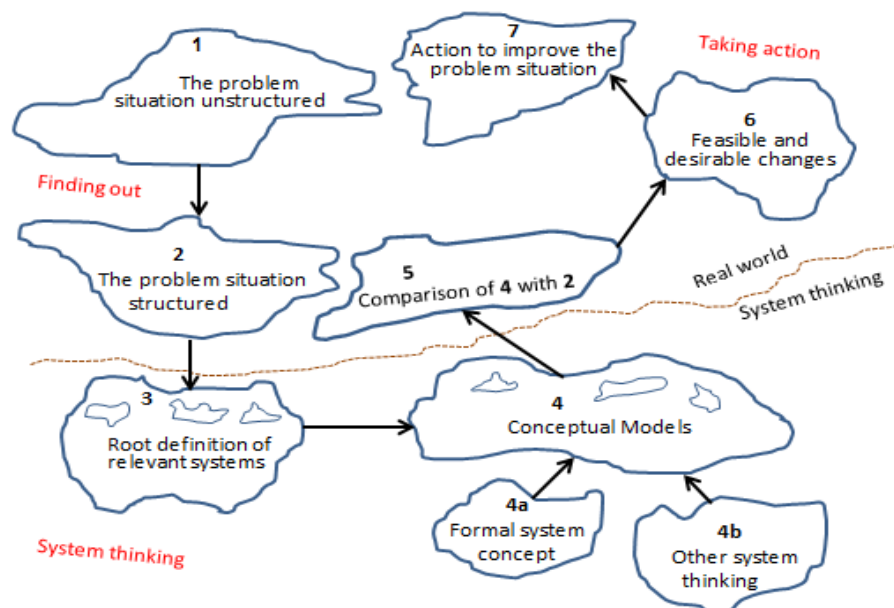


Figure 3.1: Stages of soft systems methodology

Source: (Checkland & Scholes, 1990; Checkland, 1998)

Applying the seven stages of SSM (Figure 3.1); SSM seeks to explore the ‘messy’ problematic situations that arise in human activity (Graham, 1989; Salner & Ph, 1999). It uses the concept of a system of human activity as a means to get from the ‘finding out’ of the problematic situation (wicked, complex problem) to ‘taking action’ to improve the situation (Salner & Ph, 1999; Sanga, 2010). SSM has

strengths and weaknesses. One of the strengths of SSM, it solves complex messy problematic situations involving the human factor. One of the weaknesses of SSM is that it does not deal with implementation issue(Kimble, 2008; Baskerville et al., 2009; Williams & Hof, 2014). The SSM integrated with DSR was employed in the creation of artifacts. The weaknesses of SSM were complemented by the strengths of DSR and vice versa. Figure 3.2 depicts how SSM compounded with DSR was used to address the research problem. SSM integrated with DSR was iterated in a circular fashion through research objectives RO₁, RO₂, RO₃ until the optimal solution was obtained.

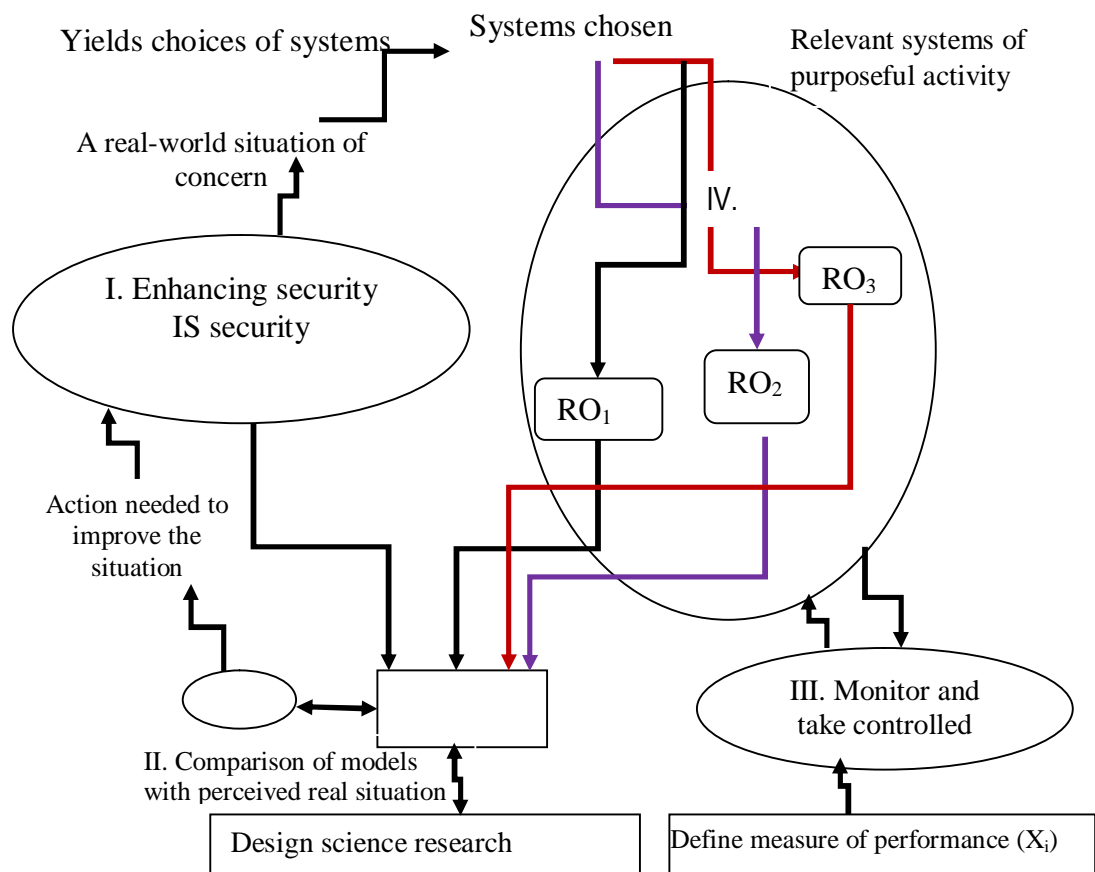


Figure 3.2: Soft systems methodology integrated with design science research

Source: adapted from Checkland & Scholes (1990), Sanga (2010)

KEY

'RO₁' stands for research activities for research objective one;

'RO₂' stands for research activities for research objective two;

'RO₃' stands for research activities for research objective three;
'X_i' stands for a measure of performance for each research objective

3.2.2 Design Science Research

Design science research (DSR) comprises of creation and evaluation of artifacts intended to solve an identified organizational problem (Hevner et al., 2004; Gregor & Hevner, 2013; Venter et al., 2015). IS artifacts are broadly defined as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems) (Futcher, 2011). DSR was employed to address the main research question, RQ3: "how to develop a framework for enhancing security information systems?" (This entails the development of IT artifacts) (Hevner et al., 2004). DSR compounded with SSM was employed in the design and development of artifact. Table 3.1 presents a summary of how DSR in conjunction with SSM was employed in this study.

Table 3.1: Applying design science compounded with soft systems methodology

S/N	Guidelines	Explanations	How DSR was applied in this study
1	Guideline 1: Design as an Artifact for ensuring the security of IS	DSR produced a viable artefact to address the research problem in the form of framework.	The viable artefacts in this study a framework for enhancing the security of IS (Section 5.4); development of a prototype to test the applicability of the developed framework for ISS (Section 5.5).
2	Guideline 2: Problem of relevance	The objective of DSR is to develop technology-based solutions to address the relevance of important business problems.	The study assessed and established IT security requirements and developed a framework to solve the organizational problem of loss of security goals (CIA triad).
3	Guideline 3: Design evaluation for artifact	The utility, quality, and efficacy of a design artifact for ensuring the security of IS were rigorously demonstrated using well-executed evaluation methods.	The evaluation was done for a developed framework for enhancing the security of IS. It was carried using SSM in conjunction with DSR by comparing the conceptual world and the real world until the optimal version. It has been published in an international journal (Published papers: Appendix F).
4	Guideline 4: Research	Effective DSR provided clear and verifiable	The research established security requirements for ensuring the security of IS;

S/N	Guidelines	Explanations	How DSR was applied in this study
	Contribution to the study	contributions in the areas of the design artifact and design methodologies.	developed a framework for enhancing the security of IS (Section 5.4).
5	Guideline 5: Research rigour for the study	DSR relied upon the application of rigorous methods in both the development and evaluation of the artifacts.	The research rigor was achieved through the use of mixed research methods and approaches in both the development, validation and evaluation of the developed artifacts (Section 5.4-5.8).
6	Guideline 6: Design as a search process for the study	The search for an effective artifact required utilizing available means to reach desired ends while satisfying laws and guidelines in the problem environment	Design as a search process was achieved through using case studies of organizations under study in the education sector in Tanzania; the study employed SSM in conjunction with DSR to compare real world and the conceptual world to get required change implementation.
7	Guideline 7: Communication of research	DSR was presented effectively to both technology-oriented and management-oriented audiences in the area under study.	The results of this study were communicated back to organizations under study in form of discussions with focused groups; published in international journals as presented in Appendix F

Source: adapted from Hevner et al.(2004)

DSR involves three closely related cycles/activities (Hevner, 2007) (Figure 3.3) out of seven guidelines (Table 3.2). The three cycles of DSR are relevance cycle, design cycle and rigor cycle (Figure 3.3). In addressing the research problem of loss of security goals (CIA triad) of IS, the three cycles of DSR were integrated into stages of SSM to create relevant innovative artifacts.

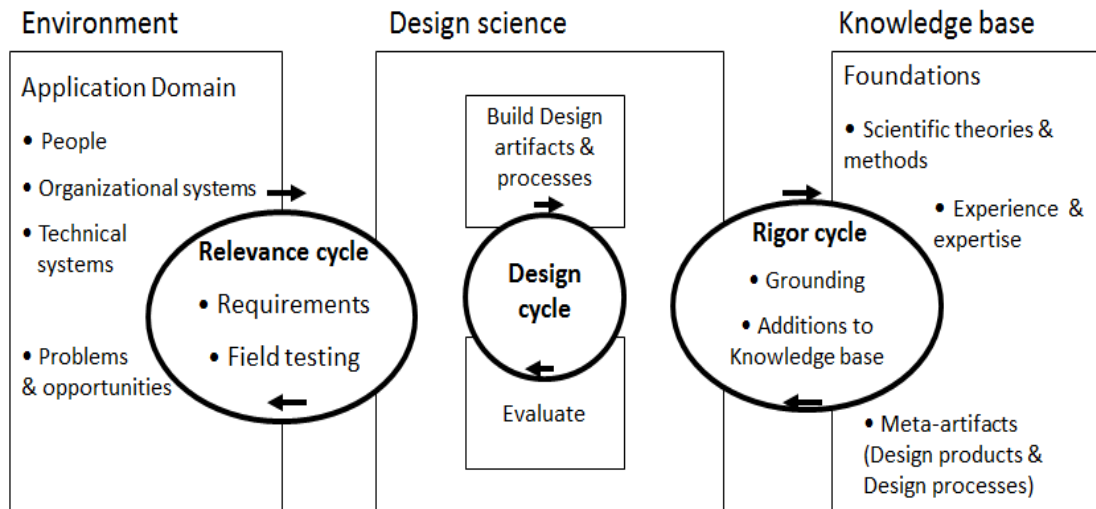


Figure 3.3: Design Science Research Cycles

Source: (Hevner, 2007)

The relevance cycle: The desire was to create relevant artifacts to solve organization problematic situation, the loss of security goals (CIA triad) of information in IS. Relevance cycle initiates DSR with an application context that provides the security requirements for the research problem to be addressed as inputs and it defines acceptance criteria for the ultimate evaluation of designed artifacts(Hevner, 2007). The relevance cycle involves field testing and feedback of developed artifacts to determine the relevance of the research problem (produce viable innovative artifact) in an iterative manner and managed by SSM in a systematic circular fashion (Checkland & Scholes, 1990; Sanga, 2010). The relevance cycle act as inputs to the design cycle for the artifacts.

Design cycle: The security requirements for innovative artifacts to tackle the research problem were determined from the relevance cycle. These security requirements from relevance cycle are input to the design cycle. The design cycle research activities iterate more rapidly between the development of an artifact, its

evaluation, and its subsequent feedback to refine the design of artifacts further. The design cycle was managed by SSM in a systematic circular fashion (Checkland & Scholes, 1990; Sanga, 2010). It involved generating design alternatives and evaluating them against security requirements from the relevant cycle until a satisfactory design was obtained (Hevner, 2007). The developed framework was subjected to rigor cycle.

Rigor cycle: The rigor cycle provided past knowledge of the study research process that ensured the created artifacts were relevant and innovative (Hevner, 2007; Gregor & Hevner, 2013). This cycle was integrated into stages of SSM which involve comparing between the conceptual world and real world to determine a desired change for the improvement (Checkland, 1990; Salner Ph, 1999; Sanga, 2010).

DSR has weaknesses and strengths. DSR is best fitted for designing and creating innovative artifacts to solve a relevant organizational problem of loss of security goals (CIA triad) for information in IS. The design is a wicked problem by itself (Farrell & Hooker, 2013) based on the following criteria: first, security requirements and constraints are unstable. Secondly, interactions among subcomponents of the problem are complex and resulting subcomponents of the solution. Thirdly, there is inherent flexibility to change artifacts and processes. Fourthly, there is a dependence on human cognitive abilities. Fifthly, there is a dependence on human social abilities. DSR has gained significant acceptance within the design work on technology solution (Gregor & Hevner, 2013) but it lacks the socio-technical concern (Baskerville et al., 2009; Mahundu, 2015, 2016) which is a vital component in the conceptualization of artifact development. In this study, the weaknesses of DSR

were complemented by the strengths of SSM and vice versa.

Table 3.2 depicts a comparison of DSR and SSM. DSR compounded with SSM was employed to solve the complex ill-defined problematic situation of loss of security goals (CIA triad) of information in IS during information states (capturing, processing, storage and transmission) in IS. This was achieved by comparing the conceptual world and the real world to obtain a desirable change for improvement (Figure 3.2, 3.3 and 3.4). This improvement required the creation of innovative artifacts to address the research problem. The developed artifact was compared with the real world in a circular fashion (Figure 3.3) until an optimal artifact was obtained.

Table 3.2: Comparison of Design Science Research and Soft Systems Methodology

Characteristic	Design science research	Soft systems methodology
Orientation	Research	Practice
Goal	Problemsolving	Problem-solving
Specificity	Generalized	Situation specific
Design role	Invention or generative	Application or (invention and application)
Outcome	Design theory or artifact is shown to have utility	Situated organizational improvement

Source: (Salner & Ph, 1999; Baskerville et al., 2009; Gregor & Hevner, 2013)

3.2.3 Integrating SSM with DSR

TheSSM was integrated with DSR (this was termed as soft design science). Razali et al. (2010) and Razali(2018) pointed out that DSR has gained significant acceptance within the design work on technology and information systems solution but it lacks the socio-technical concern which is a vital component in the conceptualization of framework development for enhancing the security of IS. Table 3.3 presents the

mapping of DSR seven guidelines and SSM seven stages during the integration process in this study.

Table 3.3: Integrating soft systems methodology with design science research

S/N	Design science research	Soft systems methodology Mapped stages
1	Guideline 1: Design as an Artifact	Stage 1-2: in stage 1 problem unstructured; Finding out, in stage 2: problem situation structured.
2	Guideline 2: Problem relevance.	Stage 3-4: system thinking; in stage 3, the root definitions of the relevant systems are defined; stage 4: a conceptual model developed.
3	Guideline 3: Design evaluation	Stages 5: Finding out, in stage 5 comparisons of conceptual models in stage 4 with the real world in stage 2 was performed.
4	Guideline 4: Research Contributions	Stage 6: Taking action; in stage 6 feasible and desirable changes were defined.
5	Guideline 5: Research rigor	Stage 7: Taking action, in stage 7 action to improve the problem situation. was executed.
6	Guideline 6: Design as a search process	
7	Guideline 7: Communication of research	

Source: adapted from Checkland & Scholes (1990); Hevner et al. (2004)

Figure 3.4 depicts how SSM was integrated with DSR in this study. Thus, by combining DSR and SSM, the weaknesses of one are complemented by the strengths of the other and vice versa.

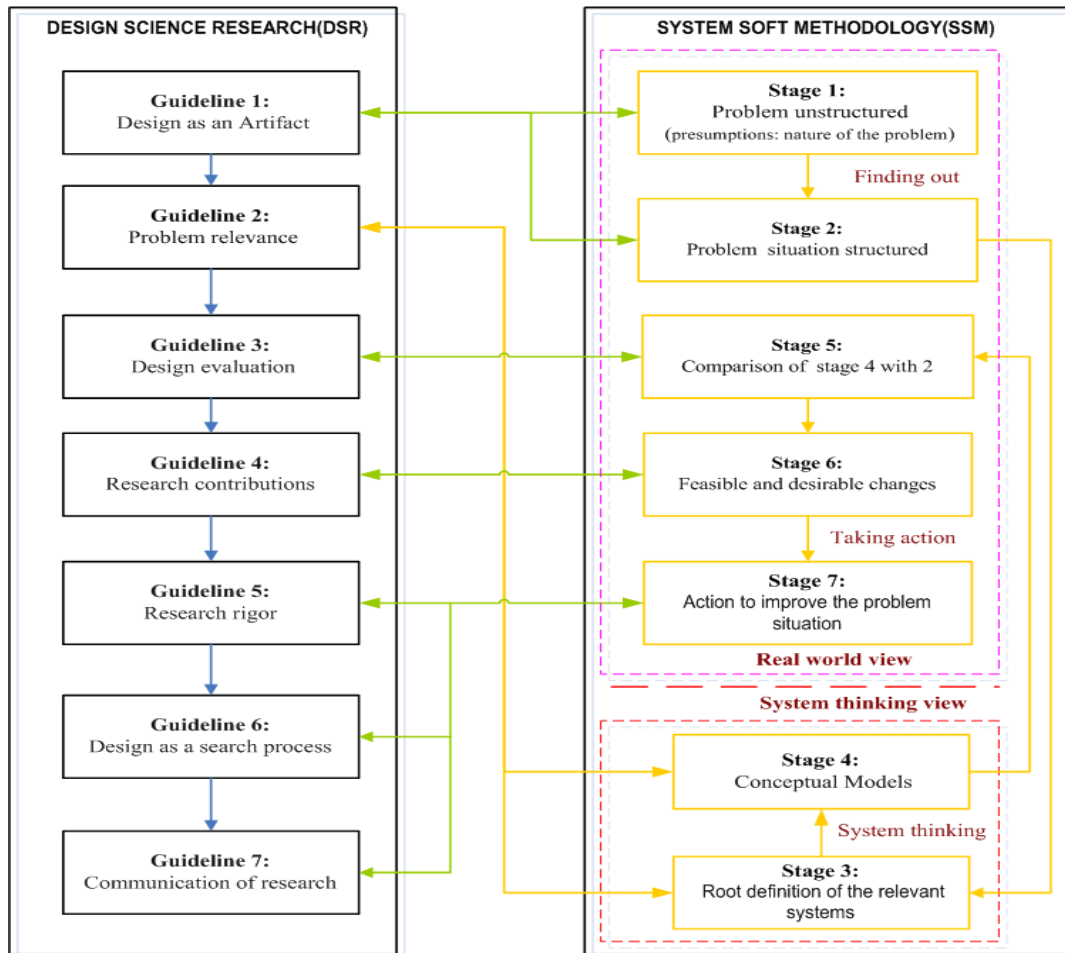


Figure 3.4: Soft Systems Integrated with Design Science Research

3.3 Research Methods

The study employed mixed research methods (qualitative and quantitative) to answer the main research problem of loss of security goals (CIA triad) for information in IS during information states in IS. The mixed research methods enabled triangulation in research methods. The research methods employed include survey, case study, and experiment. The explanation of each is as follows.

3.3.1 Survey

The study employed survey questionnaires (Section 3.5.5) for data collection to answer research questions to address the research problem, a case study of the

education sector in Tanzania. Survey method enabled the collection of a large amount of primary data about enhancing the security of IS from 154 respondents (Table 3.5) from the seven organizations (Section 3.5.1) under study. A large sample was covered during a survey for a short period of time (Saunders et al., 2009). Some of the respondents were able to remain anonymous to the researcher. The sample was divided into three categories: management staff, ICT staff and users of IS. The research questions were designed based on responded categories: questionnaire for management staff, questionnaire for ICT staff and questionnaire for users of IS (Section 3.5.5). Both quantitative and qualitative data were collected through a survey method (Section 3.5.5).

3.3.2 Case Study

The study employed a case study to find out how to enhance the security of IS during information states in IS, a case study of the education sector in Tanzania. It refers to getting an in-depth detailed understanding of the phenomenon under study (Kothari, 2004; Cohen et al., 2007; Saunders et al., 2009). The case study in this study means the context of the research study. Furthermore, it has been adopted as a research method for studying a phenomenon in its real-world environment setting. The focus of this study was to enhance the security of information during information states (capturing, processing, storage and transmission) in IS, the case of the education sector in Tanzania.

The case study is time-consuming and labour-intensive. Due to its downfalls, the study selected seven organisations which are highly responsible for managing

education in Tanzania as detailed in Section 3.5.1 to 3.5.3. This enabled to get a deep understanding of the phenomenon under study. The study employed semi-structured interview, focus group and document review. The study addressed the problematic situation of loss of security goals (CIA triad) of information in IS during information states, a case study of the education sector in Tanzania.

3.3.3 Experiments

A controlled experiment was carried out using the Open Web Application Security Project (OWASP) Zed Attack Proxy (ZAP) tool (OWASP, 2017). The results of the experiment were recorded in table template (Section 4.4). This addressed the research question 2: To what extents are the existing security controls ensure the security of information in IS? Furthermore, the experiment was carried out to validate the developed framework for enhancing the security of information systems (Section 5.6). This addressed RQ4: How to validate the developed framework for enhancing the security of information systems? The experiment results were recorded in Table E.1 in Appendix E. Moreover, the experiment was carried out to evaluate the developed framework for enhancing the security of information systems (Section 5.4). This address research question 5, RQ5: "How to evaluate the developed framework for enhancing the security of information systems?" The controlled experiments were managed by SSM.

3.4 Problem Relevance and Root Definition

The problem relevance (Hevner et al., 2004; Hevner & Chatterjee, 2012) and problem root definition (Smyth & Checkland, 1976) were determined using CATWOE analysis (Checkland & Scholes, 1990). The CATWOE analysis is the tool

developed by Smyth & Checkland (1976) as part of the SSM. CATWOE analysis is the technical analysis tool for solving complex problems. Additionally, the CATWOE analysis defines how the solution is going to affect the business and people involved in the transformation process(Smyth & Checkland, 1976; Salner & Ph, 1999).

The study employed CATWOE analysis to determine the problem relevance and root definition of the complex, messy real world problematic situation. The CATWOE is a mnemonic with 6 elements(Smyth & Checkland, 1976; Checkland & Scholes, 1990; Checkland, 1998), where:

- C: Customer/Client:** beneficiary or victim of the system's activity(individual(s)) who receive the output from the transformation.
- A: Actors:** those individuals who would DO the activities of the transformation if the system were made real System.
- T: Transformation:** the purposeful activity expressed as a transformation of input to output; the process that turns the inputs into outputs (Input ---T---> Output).
- W: Weltanschauung:** it's a German word that literally means "worldview". It is the big picture of the situation. It is the person's worldview and beliefs, which makes the **T** meaningful.
- O: Owner:** the wider system decision maker who is concerned with the performance of the system; those with the formal power to stop the transformation.
- E: Environmental constraints:** the key constraints outside the system boundary that insignificant to the system. It refers to elements outside the system which are taken as given.

The study applied the CATWOE analysis to determine the problem root definition and problem relevance by asking at least three questions. The questions asked include: what the study is trying to achieve (W)?; How(T)?; What constraints it(E) (Checkland & Scholes, 1990; Basden, 2003)?. The root definition of the problem is the way of communicating what the problem is or what the system does? It is a statement of purpose that captures the essence of the particular situation of the relevant system (Checkland & Scholes, 1990). The results of CATWOE analysis in this study are summarized in Figure 3.5.

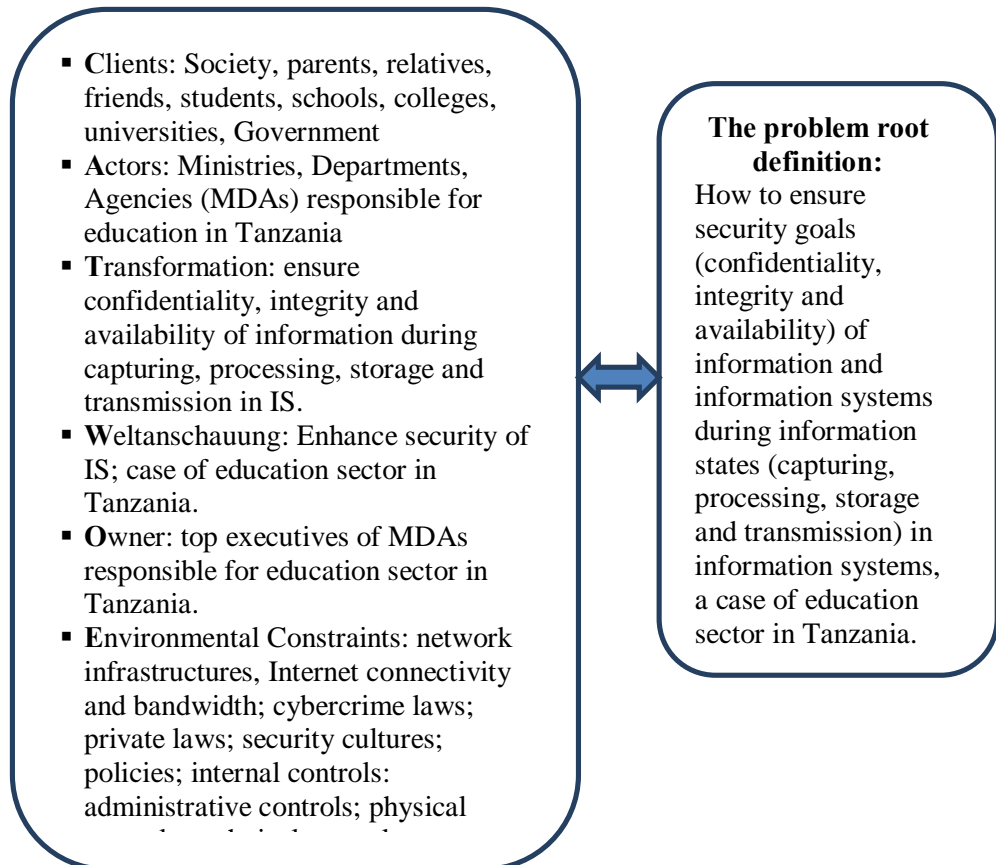


Figure 3.5: Root Problem Definition

3.5 Research Design

The research design is the conceptual structure within which research was conducted. It constitutes the blueprint for the collection, measurement, and analysis of data (Kothari, 2004; Cohen et al., 2007) to answer the research question on how to improve the security of information during information states (capturing, processing, storage and transmission) in IS.

3.5.1 Study Area

The study area for this study was the education sector in Tanzania. The selection of the education sector was based on the fact that the education sector is a strategic agent for the development of the country. It is vital for the socio-economic development of individuals, communities, and societies (MEST, 2016; Moh.go.tz, 2016; PORALG, 2016; URT, 2016). The education sector has also been selected for this study due to the fact that it is feasible to get access to data collection. Despite the various ICT initiatives in the education sector, ICT security consideration is not fully taken into account; this leads to the selection of this sector for study, aiming at bridging the identified security research gap.

The study areas in the education sector in Tanzania were the Ministry of Education, Science, and Technology (MEST, 2016); agencies and departments under the Ministry of Education, Science and Technology (MEST, 2016) and the President's Office Regional Administration and Local Government (PORALG, 2016). These study areas were selected due to their high usage of IS; and coordination role for the integration of ICT in the education sector in the country.

3.5.2 Organizations under Study

In this study, seven out of twelve organisations from the education sector (Table 1.1) were selected for the study of enhancing the security of IS. The selected organizations are K, L, M, N, O, P and Q. The organizations selected are those which are mainly involved in the educational assessment and management of education in Tanzania, because of their high impact on the whole sector.

Table 3.4: Description of the organizations under study

S/N	Organization	Description
1	Organization K	Organization K is mandated to recognize, approve, register and accredit universities operating in Tanzania and local or foreign university-level programs being offered by registered higher education institutions.
2	Organization L	Organization L is responsible for establishing the regulatory framework for technical education and training, leading to quality assured qualifications. It assists technical institutions to improve and maintain the quality of the education they provide.
3	Organization M	The main functions of organization M are to ensure responsibility for examinations within the United Republic of Tanzania and to make provision for places and centres for examinations. It acts as the body for facilitating, administering and supervising foreign examinations in the country.
4	Organization N	Organization N is charged with the responsibility of ensuring the quality of education in Tanzania at the pre-school, primary, secondary and teacher training levels. It is responsible for designing, developing, testing, reviewing and/or revising curricula at pre-primary, primary, secondary, special education and teacher training levels.
5	Organization O	The main function of organization O is to assist, on a loan basis, needy students who secure admission in accredited higher learning institutions, but who have no economic power to pay for the costs of their education. The organization O is also entrusted with the task of collecting due loans from previous loan beneficiaries in order to have a revolving fund in place so as to make the organization O sustainable.
6	Organization P	Organization P is mandated for the formulation, monitoring, and evaluation of the implementation policies, teachers' training, registration of schools, an inspection of education services and infrastructure, library services and education press services.
7	Organization Q	Organization Q has the role of coordinating, administration and management of Pre-Primary, Primary and Secondary schools.

Source: researcher, 2020

Due to the time and resources constraints, the decision of selection of seven organizations was reached and considered to be the good presentation of the entire population for the research problem under study. In this study, the names of the seven selected organizations referred to as K, L, M, N, O, P and Q were not disclosed for confidentiality purpose. In this case, the level of analysis is organizational and their explanation is given in Table 3.4.

3.5.3 The Sampling Design

Sample size depends largely on the degree to which the sample approximates the qualities and characteristics of the overall universe (Kothari, 2004; Cohen et al., 2007; Saunders et al., 2009). The research involved the collection of quantitative and qualitative data to answer research questions. The sample size for this study was 154 respondents from seven organizations in the education sector. The distributions of these respondents are presented in Table 3.5. This sample was selected using purposive and stratified random sampling techniques.

Purposive sampling relies on the judgment of the researcher when it comes to selecting the units (e.g., people, cases, organizations, events, pieces of data) that are to be studied (Kothari, 2004; Cohen et al., 2007). The selected respondents in this study were those involved in the managing of ICT and security of IS; procurement decisions of ICT equipment/accessories; ICT use and compliances. The respondents were selected based on the organization structure. Taking into account these aspects, the purposive sampling technique was the optimal choice for sampling design. The respondents (Table 3.5) were comprised of top management (Permanent Secretary, Commissioners, and Chief Executive Officers), senior management (Directors, Chief

Financial Officers, Divisions/ Head of Departments), Operations management (Head of Units, Sections), ICT experts (Network/Systems Administrators, IT Security Specialists and other IT staff); and end users (operations staff who interact with information systems and know the business processes) from the 7 organisations under study.

Table 3.5: Respondents

Respondents	Organisation							Total
	O	P	L	M	Q	K	N	
IT staff (IT experts)	4	2	3	20	4	3	3	39
Management staff	4	5	4	21	6	5	5	50
End users of information systems	2	3	4	19	5	2	4	39
Total respondents (sample)	11	12	12	74	18	13	14	154
Total actual respondents	10	10	11	60	15	10	12	128
Survey response rate%	91%	83%	92%	81%	83%	77%	86%	83%

Source: researcher, 2020

Stratified random sampling was used to select respondents for end users of information systems from the sampling frame (list of all end users of information systems for 7 organizations under study) based on research questions. The sampling frame is divided into 7 strata (stratum K, L, M, N, O, P, and Q) comprising of end users of IS from 7 organizations. The respondents from each stratum were selected using random sampling technique (Cohen et al., 2007; Saunders et al., 2009).

3.5.4 Data Collection Techniques

The study employed both quantitative and qualitative research methods for data collection which enabled triangulation to take place. The quantitative research method for data collection which was employed was surveyed questionnaire. The qualitative research methods which were employed are an interview for focused

group/individuals and document review (Cohen et al., 2007). The data collection was conducted from March 05, 2015, to January 20, 2016, in seven organizations in the education sector in Tanzania.

3.5.4.1 Survey Questionnaire

The first data collection method was a survey questionnaire. The reasons for choosing the survey questionnaire method includes avoidance of bias by the researchers; cost-effective way of collecting data, large samples can be made use of, and thus the results can be made more dependable and reliable (Kothari, 2004; Cohen et al., 2007; Saunders et al., 2009). The main demerits of this technique include a low rate of return of the duly filled in questionnaires as there is an inbuilt inflexibility because of the difficulty of amending the approach once questionnaires have been dispatched. Due to these limitations, before using this technique - the researcher(s) conducted a pilot survey to test the questionnaires (Cohen et al., 2007; Saunders et al., 2009). In this study, three different categories of survey questionnaires (management staff, ICT staff and users of IS) were used (Appendix B) for data collection. The survey data were collected from 128 participants out of 154 participants from seven organizations as presented in Table 3.5; the response rate was 83%.

3.5.4.2 Interview

The second data collection technique was a semi-structured interview. This instrument involves the presentation of oral-verbal stimuli and replies in terms of oral-verbal responses (Cohen et al., 2007; Saunders et al., 2009). The advantages of the interview instrument include the fact that more information can be obtained and

in greater depths; and non-response generally remains very low (Kothari, 2004; Cohen et al., 2007). Interview technique has weaknesses which include expensiveness especially when a large and widely spread geographical sample is taken; the possibility of the bias of interviewer as well as that of the respondent (Kothari, 2004; Saunders et al., 2009). Due to these limitations, before using this technique, the researcher(s) did prior planning before the interview and adhered to research ethics.

A semi-structured interview was conducted with 18 participants (Head of ICT and ICT experts) in seven organizations under study. Table 3.6 depicts the distribution of participants for a semi-structured interview conducted by seven organizations in the education sector in Tanzania. The study used data interview collection matrix and open-ended questions (Appendix B). The interview lasted for one hour.

Table 3.6: Summary of an interview data sample

Respondents	Organisation							Total
	O	P	L	M	Q	K	N	
Head of ICT & IT staff	1	3	2	4	4	1	3	18

3.5.4.3 Document Review

Another data collection technique employed was a document review. It is a way of collecting data by reviewing existing documents (Cohen et al., 2007). The documents may be hardcopy or electronic and may include reports, program logs, performance ratings, funding proposals, meeting minutes, newsletters, and marketing materials (Bowen, 2009). The advantages of this method include: it is relatively inexpensive; good source of background information; and provides a behind the scenes look at a program that may not be directly observable. The disadvantages of

desk or document review include information that may be inapplicable, disorganized, unavailable, or out of date; can be time-consuming to collect, review, and analyze many documents. A document review was conducted in seven organizations under study in the education sector in Tanzania. Table 3.7 depicts a summary of the reviewed documents in this study.

Table 3.7: Document review

	Document reviewed	Remarks
1	ICT policy	Desk review carried out for ICT policy for seven organization
2	Security Policy and operational manuals for IS	Desk review carried out for IT security policy for seven organization

Source: researcher, 2010

3.5.5 Designing of Survey Questionnaires

The designed survey questionnaires were of three categories namely, questionnaire for management staff (Appendix B); survey questionnaire for general staff (Appendix B); and survey questionnaire for IT staff (Appendix B). Due to the nature of the research problem, SSM in conjunction with ISO/IEC 21827:2008: the security of the system engineering-capability maturity model was adopted to guide the design of survey questionnaires in a systematic way (Checkland & Scholes, 1990; Sanga, 2010; Novani et al., 2014). ISO/IEC 21827:2008: systems security engineering-capability maturity model (SSE-CMM) was adopted to address security engineering aspects, in particular, to incorporate secure principles in system life cycles of IS (ISO/IEC 21827, 2008; Yan et al., 2011). The SSE-CMM with a rating scale of 0-5: minimum 0 and maximum 5 was used as summarized in Table 3.8.

Table 3.8: SSE-CMM Rating Scale Description

SSE-CMM rating scale	Description of a security rating scale for maturity
0-not performed (non-existent)	The organization does not recognize the need for IT security. There is a complete lack of a recognizable system security administration process.
1-Performed informally (unplanned/ad-hoc)	The organization recognizes the need for IT security. But the organization considers IT risks in an ad hoc manner, without following defined processes or policies.
2-Partially implemented (planned)	Responsibilities and accountabilities for IT security are assigned to an IT security coordinator. There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing.
3-Implementation is in progress (planned and tracked);	Security awareness exists and is promoted by management. An organization-wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.
4-Fully implemented (well defined and auditable);	Responsibilities for IT security are clearly assigned, managed and enforced. The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management.
5-Fully implemented and regularly updated (monitored and audited for compliance)	IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. Risk assessment has developed to the stage where a structured, organization-wide process is enforced, followed regularly and managed well.

Source: (ISO/IEC 21827, 2008; Yan et al., 2011)

The designed survey questionnaires (Appendix B) were designed based on the experience of past related research survey questionnaires and they were developed by adopting some questions on the past researches' questionnaires (Ismail et al., 2010; Shaaban, 2014; Educause.edu, 2015). Some questions were based on the literature review. The survey questionnaires comprise of closed research questions and open-ended questions.

3.5.6 Design of Interview Data Collection Matrix Tool

A data collection matrix tool (Appendix B) was developed based on PCI (2010), ISO/IEC 27002:2013, Beissel (2014) and literature review. The data collection matrix tool was employed in an interview for the focused group.

3.5.7 Pre-Testing and Pilot Study

The purpose of the pre-testing and pilot study was to refine the survey questionnaires so that respondents would have no problems in answering the questions, and to ensure that there would be no problem in recording the data. Thus, it enabled to obtain assessments of the questions' validity and reliability of data that would be collected. The pre-testing and pilot study activity were conducted from January 2, 2015, to February 28, 2015, in organization M involving 41 respondents.

3.6 Access and Research Ethics

The researcher(s) signed confidentiality declaration form (Appendix I) issued by the Directorate of Research, Publications and Postgraduate studies endeavours of OUT. Ethical issues considered in this study were included in the survey questionnaires to inform them about the privacy and confidentiality of information they would provide to researchers. The results of this study were published without revealing the particulars of the participants.

3.7 Data Analysis

3.7.1 Data Analysis Techniques

The data collected were analyzed using qualitative and quantitative techniques. The qualitative data were cleaned, coded, transcribed and analyzed. The quantitative data

were analyzed using the R statistical computing package. R is a software language for carrying out complicated (and simple) statistical analyses (Beaujean, 2013; Fox, 2015).

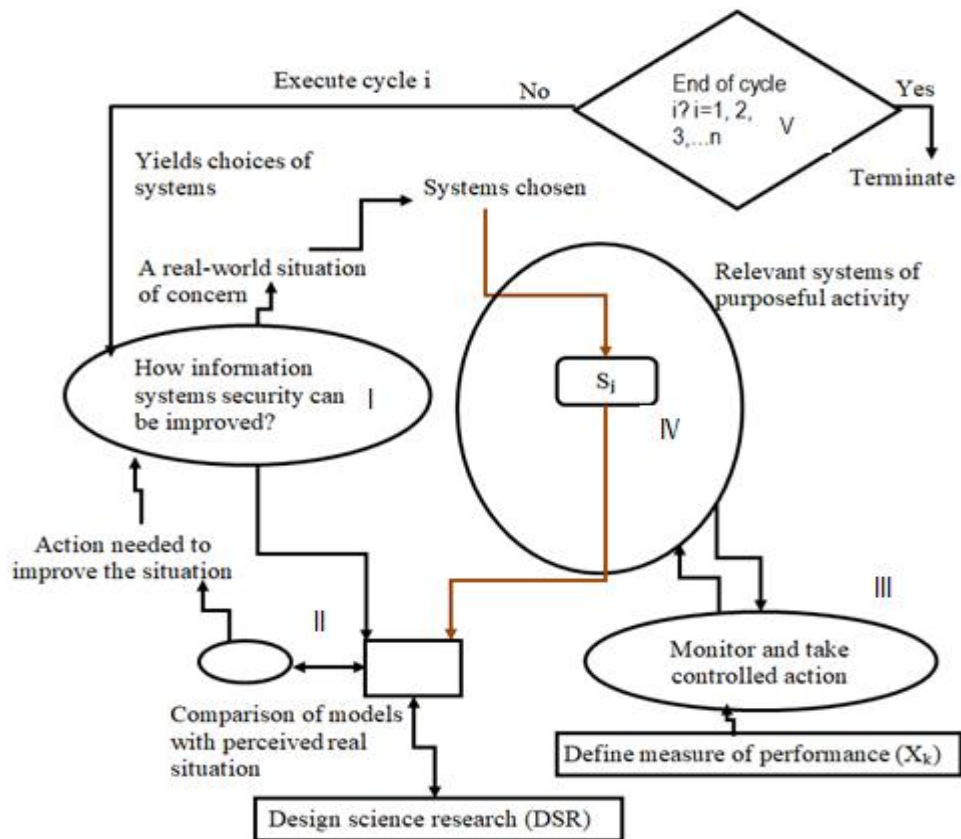


Figure 3.6: Soft Systems Methodology integrated with Design Science Research

Source: Adapted from Salner & Ph (1999); Sanga (2010)

KEY

S_j is the collected data based on category (for example, IT staff, management staff, the user of IS).

The choice of R was based on the nature of research questions; data collections techniques, methods adopted the nature of data that were collected; and the capability of R in comparison with other statistical data analysis computing packages. The data collected were coded and summarized in a relational database (Appendix C). The data collected through survey questionnaires and data matrix

collection tool were based on SSE-CMM(ISO/IEC 21827, 2008)with a rating scale of 0-5 (Figure 3.6).

Collected data were first cleaned and coded before being analyzed. In cycles $i=1, 2, 3, \dots, n$ (Figure 3.6).The analysis was done in cycle $i=1$ for management staff ($S_j, j=1$); cycle $i=2$ for IT staff ($S_j, j=2$); cycle $i=3$ for end user of information systems ($S_j, j=3$). Out of these comparisons give relevance systems of purpose which require improvement.

3.7.2 Statistical Data Analysis of Collected Data

The data analysis employed both descriptive statistics and non-parametric statistical methods to determine the significance of each variable for enhancing the security of IS based on research questions. The statistical data analysis method employed was the Chi-Square Goodness of Fit Test (χ^2)(Kothari, 2004). This is given by equation 3.1.

$$\chi^2(df) = \sum_i^N \frac{(O_i - E_i)^2}{E_i} \quad \text{Equation 3.1.}$$

In equation 3.1 df is the degree of freedom; O_i is the observed frequency for each category i ; E_i is the expected frequency for each category i . In this study, the category $i=0, 1, 2, 3, 4, 5$; it is based on SSE-CMM. Where N is the total number of observation in the sample size of respondents category under study. Thus, for k categories, $df = k - 1$; $\sum O_i = \sum E_i = N$; $E_i = Np_i$; $p_i = \frac{1}{k}$; $\sum p_i = 1$; where p_i is proportional of expected frequency for category i in k categories. In this study,

expected frequency E_i and observed frequency O_i . The null and alternative hypotheses were stated as follows.

$H_0 : O_i = E_i$ The variable x_i for security measures or security controls do not contribute to enhancing the security of IS

$H_1 : O_i \neq E_i$ The variable x_i for security measures or security controls contribute to enhancing the security of IS

Where H_0 and H_1 denotes the null hypothesis and the alternative hypothesis respectively. The hypotheses were tested at 95% confidence interval, significance level $\alpha = .05$.

The choice of the Chi-Square Test was chosen due to the nature of the research questions and the nature of research data collected (Table 3.5). The Chi-square test in this study satisfied the following assumptions.

- i. First assumption: The variable under study involves six categorical ordinal variables, the SSE-CMM rating scale of 0-5: minimum is 0 and the maximum is 5. The expected probability proportions for each of the six categories are equally distributed.
- ii. Second assumption: the research study was having the independence of observations as there was no relationship between the cases observed (For example participant: management staff, IT staff and users of IS).
- iii. Third assumption: the groups of the categorical variable must be mutually exclusive. For example, if the six groups of a categorical variable in SSE-CMM as defined in Table 3.8. Thus, a case, for example, a participant in the IT

Staff case category could only be in one of these six groups. For example, a participant could not have been classified in SSE-CMM as 0-not performed and 5-fully implemented and regularly updated, but only one or the other.

- iv. Fourth assumption: there must be at least 5 expected frequencies in each group of the categorical variable (0-5). This research data analyzed satisfies all of the four assumptions required by Chi-Square Goodness of Fit test.

3.8 Validity and Reliability

Validity is concerned with whether research findings are really about what they appear to be (Kane, 2001; Golafshani, 2003; Drost, 2011). Validity is the extent to which any measuring instrument measures what it is intended to measure or how truthful the research results are (Thatcher, 2010; Drost, 2011). Threats to validity include testing and mortality. This refers to participants dropping out of studies. Moreover, threats to validity include maturation which refers to change due to ageing or development, either between or within groups (Haynes et al., 1995; Golafshani, 2003; Thatcher, 2010). In this research, the stated threats above were addressed accordingly.

The validity can be classified as content validity and discriminant validity. The content validity refers to the extent to which the items are a good measure of the domain of each variable (Kane, 2001; Drost, 2011). This is undertaken essentially by judgment. The discriminant validity: this refers to the extent to which a concept differs from others (Clark & Watson, 1995; Golafshani, 2003; Drost, 2011). A series of different research questions were designed and administered to three different groups: management, IT staff and users of IS. The triangulation of data and methods

were employed to ensure the validity of this research. The result findings were compared with other similar works to see their agreements.

Reliability is the extent to which the measurements of a test remain consistent over repeated tests of the same subject under identical conditions (Davey et al., 2010; Thatcher, 2010; Tavakol & Dennick, 2011). The data collection instruments design was based on SSE-CMM rating scale 0-5 and was managed by SSM. In this study, reliability and validity were taken into considerations during the design of data collection tools; data collections and data analysis by employing mixed researches.

CHAPTER FOUR

FINDINGS

4.1 Introduction

4.1.1 General Introduction

This chapter presents the results of research findings. It first presents an overview of how the data were collected and analysed. The results findings are presented according to research objectives and research questions; and organized in sections as follows. Section 4.2 presents the research findings on security measures for ensuring security goals (confidentiality, integrity and availability) for information in IS during information states. Section 4.3 presents the research findings of security controls in each security domain. Section 4.4 presents research findings on the assessment of existing security controls using a controlled experiment. Finally, section 4.5 presents research findings of assessment for improving the security of information in IS, a case study of the education sector in Tanzania.

4.1.2 Overview of Data Analysis

The collected data were cleaned, coded and analysed using both descriptive statistics and non-parametric statistical methods to determine the significance of each variable for enhancing the security of IS based on research questions. The statistical data analysis method employed was the Chi-Square Goodness of Fit Test (χ^2) at a 95% confidence interval (Section 3.7.2). The main research problem addressed in this study was the loss of security goals (CIA triad) for information in IS during information states in IS, a case of the education sector in Tanzania. The data were collected using a survey questionnaire, semi-structured interview (using interview

data collection matrix and open interview questions), and document review as summarized in Table 4.1.

Table 4.1: Research Questions and Data Collection Tools Mapping

Research Objectives (RO)	Research questions(RQ)	Data collection tools	Items (Questions)
RO ₁ : To assess the existing security measures for ensuring confidentiality, integrity, and availability of information in information systems	RQ ₁ : To what extents are the existing security measures ensure confidentiality, integrity and availability of information in information systems?	Survey questionnaire for management staff (Appendix B)	Question v, x, xi, xii
		Survey questionnaire for general staff (Appendix B)	Question iv, vii, viii, ix, xi-xviii
		Survey questionnaire for IT staff (Appendix B)	Question 1, 2, & 3
RO ₂ : To assess the existing security controls for ensuring the security of information in information systems	RQ ₂ : To what extents are the existing security controls ensure the security of information in information systems?	Survey questionnaire for management staff (Appendix B)	Question i-iv, vi-ix
		Survey questionnaire for general staff (Appendix B)	Question i, ii, iii, v,vi, x
		Survey questionnaire for IT staff (Appendix B)	(Question 4)
		Interview Data Collection Matrix Tool (Appendix B)	Part B: Question 1, 2, 3, 5, 6
		Controlled experiment	Research question 2
RO ₃ : To develop a framework for enhancing security information systems	RQ ₃ : How to develop a framework for enhancing the security of information systems?	<ul style="list-style-type: none"> •Interview Data Collection Matrix Tool (Appendix B) •Document review 	Part A: Item1-15; Part B: Question 4
RO ₄ : To validate the developed framework for enhancing the security of information systems	How to validate the developed framework for enhancing the security of information systems?	<ul style="list-style-type: none"> •Develop an algorithm for enhanced security based on cryptographic techniques •Develop Java Prototype based on developed algorithm •Performance analysis using simulation controlled experiment 	
RO ₅ : To evaluate the developed framework for enhancing the security of information and information systems	How to evaluate the developed framework for enhancing the security of information and systems?	<ul style="list-style-type: none"> •Controlled simulation experiment •Post survey questionnaire 	

Source: researcher, 2010

This research specifically administered survey questionnaires to IT staff (41 questionnaires were distributed), users of IS (53 questionnaires were distributed) and management staff (60 questionnaires were distributed) to seven organizations in Tanzania education sector. The overall response rate was 83% as shown in Table 3.5. The ICT staff respondents' education profile majority (84.7%) of them were graduate of the first degree and postgraduate degrees as shown in Table C.1. Further, the research employed semi-structured interview to IT experts (Head of ICT, IT staff) of seven organizations under study using an interview data collection matrix tool (Appendix B); and document review (Section 3.5.4.3) from seven organizations under study.

Due to the nature of the research problem, SSM (Figure 3.6) in conjunction with ISO/IEC 21827:2008: SSE-CMM (Table 3.8) was adopted to guide the management of the analysis of data in a systematic way (Checkland & Scholes, 1990; Sanga, 2010; Novani et al., 2014). The SSE-CMM was employed to address security engineering aspects, in particular, to enable secure principles are incorporated in all system security life cycles of IS. The SSE-CMM, with a rating scale of 0-5: minimum 0 and maximum 5 (as detailed in Table 3.8).

The collected data were coded; analyzed using R Statistical computing, and ISS analysis tool. The analysis of the collected data was managed by SSM integrated with DSR (Figure 3.6) in four cycles. The first cycle involved the analysis of a survey questionnaire for IT staff. The second cycle involved the analysis of a survey questionnaire for users of IS staff. The third cycle involved the analysis of a survey questionnaire for management staff. The fourth cycle involved the analysis of

qualitative data: which were collected through a semi-structured interview and document review in seven organizations under the study. The research findings of each cycle have been presented according to research objectives. The findings are presented as follows.

4.2 Security Measures for Ensuring Security Goals

The objective was to assess the existing security measures for ensuring confidentiality, integrity, and availability of information in IS. This section addresses the research question, RQ₁: To what extents are the existing security measures ensure confidentiality, integrity and availability of information and information systems? The survey data were analysed from a survey questionnaire for management staff: question v, x, xi, xii (Appendix B); survey questionnaire for general staff: question iv, vii, viii, ix, xi-xviii (Appendix B), and survey questionnaire for IT staff: question 1, 2, & 3 (Appendix B). The survey data collected and analyzed were from 128 respondents out of 154 respondents from seven organizations under study with a response rate of 83 % as shown in Table 4.2. The collected data were cleaned, coded, entered into the analysis database (Appendix C) and analyzed using R-statistical computing. The result findings for security measures for ensuring the confidentiality, integrity, and availability of information in IS are presented as follows.

4.2.1 Measures for Ensuring Confidentiality of Information

This section addresses part of the research question (RQ₁): To what extents are the existing security measures confidentiality, integrity and availability of information and information systems? This research question was addressed through a research

study to assess the existing security measures for ensuring the confidentiality of the information in IS, a case study of the education sector in Tanzania. The findings for security measures for ensuring the confidentiality of information in IS are presented below.

4.2.1.1 Identification and Authentication

Unique user account and password for accessing IS

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine the significance level contributions of using a unique user account and password to ensure confidentiality of information in IS. It was hypothesized that the use of a unique user account and password for accessing IS contributes to ensuring the confidentiality of information in IS.

Table 4.3 depicts the views when respondents were asked whether every employee in a given organization have a unique user account and password for accessing IS. The findings depicted that the majority of respondents (61.5%: IT staff) revealed that the use of unique user account and password for every employee for accessing IS have been implemented in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.3). Moreover, the Chi-square goodness of fit test ($\chi^2(5, N = 39) = 63.923, p < .05$) in Table 4.3 revealed that the use of unique user account and password for accessing IS contributes to ensuring the confidentiality of information in IS. Thus, in ensuring the confidentiality of information, every employee in a given organization should have a unique user account and password for accessing IS.

Table 4.3: Unique user account and password for accessing information systems

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	2	5.1
1-Performed informally (unplanned)	24	61.5
2-Partially implemented (planned)	9	23.1
3-Implementation is in progress (planned and tracked)	2	5.1
5-Fully implemented and regularly updated (monitored and audited for compliance)	2	5.1
Total	39	100.0
Median=1; $E_i=1/6*39=6.5$		
$\chi^2(df = 5) = 63.923$; $p = .000$; significance level = .05		
$\sum E_i = \sum O_i = N = 39$		

Using Smartcards for accessing IS

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine the significance level contributions of ensuring the confidentiality of IS by using smartcards for accessing IS. It was hypothesized that the use of smartcards for accessing IS contribute to ensuring the confidentiality of information in IS. Table 4.4 depicts the views when respondents were asked whether employees in a given organization use smartcards for accessing IS (e.g. login to the domain, accessing applications). The findings portrayed that, the majority of respondents (100%: IT staff) revealed that organizations do not use a smartcard for accessing IS (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.4). As shown in Table 4.4, the Chi-square goodness of fit test ($\chi^2(5, N = 39) = 195.000$, $p < .05$) revealed that the use of smartcard for accessing IS contribute to ensuring the confidentiality of information in IS. Thus, in ensuring the confidentiality of information, organizations should use smartcard (something one can own) for accessing IS.

Table 4.4: Smartcards for Accessing Information Systems

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	39	100.0
Median = 0; E_i per category $i=1/6*39=6.5$		
$\chi^2 (df = 5) = 195.000; p = .000$		
$\sum E_i = \sum O_i = N = 39$		

Physical lock keys and smartcards/biometric authentication

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine the significance level contributions of using physical lock keys and smartcards/biometric authentication to access data sensitive areas in ensuring the confidentiality of IS. It was hypothesized that the use of physical lock keys and smartcards/biometric authentication to access data sensitive areas contribute to ensuring the confidentiality of information in IS.

Table 4.5 depicts the views when respondents were asked whether the organization use physical lock keys and smartcards/biometric authentication to access data sensitive areas (e.g. server rooms/data centre, network termination rooms). The majority of respondents (59%: IT staff) revealed that organizations do not use physical lock keys and smartcards/biometric authentication to access sensitive data are as (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.5). A similar question was asked to the management staff on whether employees in an organization use physical lock keys and smartcards/biometrics to access their offices. The majority of respondents (94%: management staff) revealed that organizations do not use physical keys lock and smartcards/biometric authentication to access their offices (scale 0 with a median of 0 in SSE-CMM rating scale of 0-5). A similar question was asked to users to IS staff on whether they access their office through a

door that has a physical key lock and smartcard/biometric authentication. The majority of the respondents (95%: ISuser staff) revealed that organizations do not use physical lock keys and smartcards/biometric authentication to access their offices (scale 0 with a median of 0 in SSE-CMM rating scale of 0-5).

Table 4.5: Physical lock keys and smartcards/biometric

SSE-CMM level	Observed N	Percent
IT staff: Physical lock keys and smartcards/biometric		
0-Not performed (non-existent)	23	59.0
1-Performed informally (unplanned)	15	38.5
2-Partially implemented (planned)	1	2.6
Total	39	100.0
Median = 0; E_i per category $i=1/6*39=6.5$ $\chi^2(df = 5) = 77.154$; $p = .000$ $\sum E_i = \sum O_i = N = 39$		
Management staff: Physical lock keys and smartcards/biometric		
0-Not performed (non-existent)	47	94.0
1-Performed informally (unplanned)	3	6.0
Total	50	100.0
Median = 0; E_i per category $i=1/6*50=8.3$ $\chi^2(df = 5) = 216.160$; $p = .000$ $\sum E_i = \sum O_i = N = 50$		
Users of IS: Physical lock keys and smartcards/biometric		
0-Not performed (non-existent)	38	97.4
1-Performed informally (unplanned)	1	2.6
Total	39	100.0
Median = 0; E_i per category $i=1/6*39=6.5$ $\chi^2(df = 5) = 183.308$; $p = .000$; $\sum E_i = \sum O_i = N = 39$		

As shown in Table 4.5, the Chi-square goodness of fit test results for all of the three categories of respondents (IT staff: $\chi^2(df = 5) = 77.154$; $p < .05$; management staff: $\chi^2(df = 5) = 216.160$, $p < .05$; users of IS: $\chi^2(df = 5) = 183.308$; $p < .05$) revealed that the use of physical lock keys and smartcards/biometric authentication to access their

offices contributes to ensuring the confidentiality of information. Thus, in ensuring the confidentiality of information, organizations should use physical lock keys and smartcards/biometric authentication for accessing sensitive data areas (e.g. server rooms/data centre and network termination rooms).

4.2.1.2 Access Controls Mechanisms for Confidentiality

Technologies to block or restrict unencrypted sensitive information

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine the significance level contributions of using technologies (e.g. Firewalls, Access Control Lists (ACLs)) to block or restrict unencrypted sensitive information from travelling to untrusted networks such as the Internet. It was hypothesized that the use of technologies (e.g. Firewalls, Access Control Lists (ACLs)) to block or restrict unencrypted sensitive information from travelling to untrusted networks such as the Internet, contribute to ensuring the confidentiality of information in IS.

Table 4.6 depicts the views when respondents were asked whether a given organization uses technologies (e.g. Firewalls, Access Control Lists (ACLs)) to block or restrict unencrypted sensitive information from travelling to untrusted networks such as the Internet. The findings depicted that, the majority of respondents (84.6%: IT staff) revealed that organizations have implemented in ad-hoc the use of technologies to block or restrict unencrypted sensitive information from travelling to untrusted networks(scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5(Table 4.6). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 132.538, p < .05$) in Table 4.6 revealed that the use of

technologies (e.g. Firewalls, Access Control Lists (ACLs)) to block or restrict unencrypted sensitive information from travelling to untrusted networks such as the Internet, contribute to ensuring confidentiality of information in IS. Thus, in ensuring the confidentiality of information, organizations should use technologies such as firewall, ACLs to block or restrict unencrypted sensitive information from travelling to untrusted networks.

Table 4.6: Technologies to block or restrict unencrypted sensitive data

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	5	12.8
1-Performed informally (unplanned)	33	84.6
5-Fully implemented and regularly updated (monitored and audited for compliance)	1	2.6
Total	39	100.0
Median = 1; E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 132.538$; $p = .000$, $\sum E_i = \sum O_i = N = 39$		

Classification of information resources

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine the significance level contributions to classifying information resources (assets) by indicating access levels (public, confidential, secret) and documenting them contribute to ensuring the confidentiality of information in IS. It was hypothesized that classifying information resources (assets) by indicating access levels (public, confidential, secret) and documenting them contribute to ensuring the confidentiality of information in IS.

Table 4.7 depicts the views when respondents were asked whether organizations classify information resources (assets) by indicating access levels (public,

confidential, secret) and are documented. The findings depicted that, the majority of respondents (79.5%: IT staff) revealed that organizations classify information resources by indicating access levels and document them in an ad-hoc manner (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.7). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 118.692, p < .05$) in Table 4.7 revealed that classifying information resources (assets) by indicating access levels (public, confidential, secret) and documenting them contribute to ensuring the confidentiality of information in IS. Thus, in ensuring the confidentiality of information, organizations should classify and document information resources by indicating access levels (public, confidential, secret).

Table 4.7: Classifying information resources: public, confidential, secret

SSE-CMM	Observed N	Percent
0-Not performed (non-existent)	8	20.5
1-Performed informally (unplanned)	31	79.5
Total	39	100.0
Median = 1; E_i per category $i = 1/6 * 39 = 6.5$, $\chi^2(df = 5) = 118.692$; $p = .000$, $\sum E_i = \sum O_i = N = 39$		

The access control mechanism for authorizing and revoking access rights

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine the significance level contributions of the use of access control mechanisms (role-based, user rights, access control lists) for authorizing and revoking access rights for users to IS, and documenting them, contributes in ensuring confidentiality of information in IS. It was hypothesized that the use of access control mechanism (role-based, user rights, access control lists) for authorizing and

revoking access rights for users to IS, and by documenting them, contribute in ensuring the confidentiality of information in IS.

Table 4.8 depicts the views when respondents were asked whether a given organization has access control mechanism (role-based, user rights, access control lists) for authorizing and revoking access rights for users to IS, and it is documented. The findings depicted that, the majority of respondents (79.9%: IT staff) revealed that organizations have ad-hoc access control mechanisms for authorizing and revoking access rights to IS (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.8). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 106.385, p < .05$) in Table 4.8 revealed that use of access control mechanism (role-based, user rights, access control lists) for authorizing and revoking access rights for users to IS, and by documenting them, contribute in ensuring confidentiality of information in IS. Thus, ensuring the confidentiality of information, organizations should have access control mechanisms for authorizing and revoking access rights to IS, and it should be documented.

Table 4.8: Access Control Mechanism: Authorizing And Revoking Access

SSE-CMM	Observed N	Percent
0-Not performed (non-existent)	6	15.4
1-Performed informally (unplanned)	30	76.9
2-Partially implemented (planned)	3	7.7
Total	39	100.0
Median = 1; E_i per category $i = 1/6 * 39 = 6.5$, $\chi^2(df = 5) = 106.385; p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.1.3 Segmentation of the Network

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to

determine whether networks segmentations (subnets, VLANs) for providing different levels of security based on the information's classification (public, confidential, secret) contributes in ensuring the confidentiality of information in IS. It was hypothesized that the use of networks segmentations (subnets, VLANs) for providing different levels of security based on the information's classification (public, confidential, secret) contributes in ensuring the confidentiality of information in IS.

Table 4.9 depicts the views when respondents were asked whether organizations have implemented networks segmentations (subnets, VLANs) to provide different levels of security based on the information's classification (public, confidential, secret). The findings portrayed that, the majority of respondents (69.2%: IT staff) revealed that organizations have not implemented networks segmentations (scale 0) or they implement in ad-hoc (scale 1 unplanned); with a median of 0 in SSE-CMM rating scale of 0-5 (Table4.9).

Table 4.9: Network Segmentation: Subnets, VLAN

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	17	43.6
1-Performed informally (unplanned)	10	25.6
2-Partially implemented (planned)	12	30.8
Total	39	100.0
Median = 1 ; E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 43.000$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 43.000$, $p < .05$) in Table 4.9 revealed that the use of networks segmentations (subnets, VLANs) for providing different levels of security based on the information's classification (public, confidential, secret) contributes in ensuring the confidentiality

of information in IS. Thus, in ensuring the confidentiality of information, organizations should segment their networks (subnets, VLANs) to provide different levels of security based on the information's classification (public, confidential, secret).

Protecting servers by more than one security layer: DMZ, IDS, IPS, firewalls

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine whether protecting Internet-accessible servers with more than one security layer contributes to ensuring the confidentiality of information in IS. It was hypothesized that protecting Internet-accessible servers with more than one security layer contributes to ensuring the confidentiality of information in IS.

Table 4.10 depicts the views when respondents were asked whether Internet-accessible servers in a given organization are protected by more than one security layer: demilitarized zone (DMZ), firewalls, intrusion detection system (IDS), intrusion prevention system (IPS). The findings depicted that, the majority of respondents (76.9%: IT staff) revealed that organizations protect their Internet-accessible server with more than one security layer in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.10).

Table 4.10: Protecting servers by more than one security layer

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	6	15.4
1-Performed informally (unplanned)	30	76.9
2-Partially implemented (planned)	3	7.7
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 106.385, p = .000$, $\sum E_i = \sum O_i = N = 39$		

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 106.385, p < .05$) in Table 4.10 revealed that protecting Internet-accessible servers with more than one security layer contributes to ensuring the confidentiality of information in IS. Thus, ensuring the confidentiality of information, organizations should protect their Internet-accessible servers with more than one security layer: DMZ, firewalls, IDS, IPS.

4.2.1.4 Encryption of Information

Encryption of information during transmission and processing

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether encryption of sensitive information during transmission/processing in IS contributes to ensuring the confidentiality of information in IS. It was hypothesized that encryption of sensitive information during transmission/processing in IS contributes to ensuring the confidentiality of information in IS contributes to ensuring the confidentiality of information in IS.

Table 4.11 depicts the views when respondents were asked whether organizations encrypt sensitive data/information during transmission/processing in IS. For example

use of VPN, SSL/TLS, https, ftps for online services through untrusted networks such as the Internet. The findings depicted that, the majority of respondents (74.4%: IT staff) revealed that organizations do not encrypt sensitive data/information during transmission in IS (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.11). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 105.769, p < .05$) in Table 4.11 revealed that encryption of sensitive information during transmission/processing in IS contributes in ensuring the confidentiality of information in IS. Thus, ensuring the confidentiality of information, organizations should encrypt sensitive data/information during transmission and processing in IS.

Table 4.11: Encryption of Data During Transmission/Processing

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	29	74.4
1-Performed informally (unplanned)	10	25.6
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 105.769, p = .000$, $\sum E_i = \sum O_i = N = 39$		

Encryption of data, information during storage

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether encryption of data during storage (backups, storage over network/fileserver(s), databases) contributes in ensuring the confidentiality of information in IS. It was hypothesized that encryption of data during storage (backups, storage over network/fileserver(s), databases) contributes to ensuring the confidentiality of information in IS.

Table 4.12 depicts the views when respondents were asked whether a given organization do encrypt data during storage (backups, storage over network/fileserver(s), databases). The findings portrayed that, the majority of respondents (100%: IT staff) revealed that organizations do not encrypt data/information during storage in IS (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.12). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 195.000, p < .05$) in Table 4.12 revealed that encryption of data during storage (backups, storage over network/fileserver(s), databases) contributes in ensuring the confidentiality of information in IS. Thus, in ensuring the confidentiality of information, organizations should encrypt data/information during storage (backups, storage over network/fileserver(s), databases) in IS.

Table 4.12: Encryption of data during storage

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 195.000, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.1.5 Media-Sanitization: Destroy Data Permanently

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether implementation of a media-sanitization process (delete/destroy data permanently) to equipment (e.g. computers, routers, switches, firewalls, IDS, IPS, etc.) prior to disposal, reuse, or release contributes in ensuring confidentiality of information in IS. It was hypothesized that implementation of a media-sanitization process (delete/destroy data permanently) to equipment (e.g. computers, routers,

switches, firewalls, IDS, IPS, etc.) prior to disposal, reuse, or release contributes in ensuring the confidentiality of information in IS.

Table 4.13 depicts the views when respondents were asked whether a given organization has a media-sanitization process (delete/destroy data permanently) to equipment (e.g. computers, routers, switches, firewalls, IDS, IPS, etc.) prior to disposal, reuse, or release. The findings depicted that, the majority of respondents (89.7 %: IT staff) revealed that organizations do not have a media-sanitization process for destroying data permanently from data storages, prior to disposal of ICT equipment (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.13). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 151.923, p < .05$) in Table 4.13 revealed that implementation of a media-sanitization process (delete/destroy data permanently) to equipment (e.g. computers, routers, switches, firewalls, IDS, IPS, etc.) prior to disposal, reuse, or release contributes in ensuring confidentiality of information in IS. Thus, in ensuring the confidentiality of information, organizations should have a media-sanitization process for destroying data permanently from data storages; prior to the disposal of ICT equipment.

Table 4.13: Media-Sanitization: Destroy Data Permanently

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	35	89.7
1-Performed informally (unplanned)	4	10.3
Total	39	100.0
Median = 0, E_i per category $i = 1/6 * 39 = 6.5$, $\chi^2(df = 5) = 151.923, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.1.6 Disabling, Blocking Insecure Services, Protocols, and Ports

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether identifying, disabling and blocking of all insecure services, protocols, and ports; and implementation of security features for each identified service contributes in ensuring the confidentiality of information in IS. It was hypothesized that identifying, disabling and blocking of all insecure services, protocols, ports; and implementation of security features for identified service contributes to ensuring the confidentiality of information in IS.

Table 4.14 depicts the views when respondents were asked whether a given organization identify, disable, block all insecure services, protocols, and ports; and implement security features for each identified service (examples of insecure services, protocols, or ports include FTP, Telnet, POP3, IMAP, http, and SNMP, etc.). The findings portrayed that, the majority of respondents (66.7%: IT staff) revealed that organizations identify insecure services, protocols, and ports in ad-hoc, and they implement security features for each identified service in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM scale of 0-5 (Table 4.14).

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 91.000, p < .05$) in Table 4.14 revealed that identifying, disabling and blocking of all insecure services, protocols, ports; and implementing security features for identified service contributes in ensuring the confidentiality of information in IS. Thus, in ensuring the confidentiality of information, organizations should identify, disable, and block all insecure services, protocols and ports. Organizations should implement security features for each identified service.

Table 4.14: Insecure Services, Protocols, and Ports

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	13	33.3
1-Performed informally (unplanned)	26	66.7
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 91.000$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.1.7 Patch Management for Anti-Malware, OS, IS, and ICT Devices

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether implementing a process for checking updates such as current updates/patches for antivirus software, operating systems (OS), patch level of devices (computers, routers, switches, security devices: firewall, IDS, IPS, etc.) as they connect to your network contributes in ensuring confidentiality of information in IS. It was hypothesised that implementing a process for checking updates such as current updates/patches for antivirus software, OS, patch level of devices (computers, routers, switches, security devices: firewall, IDS, IPS, etc.) as they connect to your network contributes in ensuring the confidentiality of information in IS.

Table 4.15 depicts the views when respondents were asked whether a given organization has a process for checking updates such as current updates/patches for antivirus software, OS, patch level of devices (computers, routers, switches, security devices: firewall, IDS, IPS, etc.) as they connect to your network. The findings depicted that, the majority of respondents (79.5%: IT staff) revealed that organizations update anti-virus (anti-malware) or patch there is in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.15).

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 118.692, p < .05$) in Table 4.15 revealed that implementing a process for checking updates such as current updates/patches for antivirus software, OS, patch level of devices (computers, routers, switches, security devices: firewall, IDS, IPS, etc.) as they connect to your network contributes in ensuring confidentiality of information in IS. Thus, in ensuring the confidentiality of information, organizations should have a process for checking updates and updating anti-malware, OSs, IS and ICT devices.

Table 4.15: Updates or Patches: Antivirus/OS

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	8	20.5
1-Performed informally (unplanned)	31	79.5
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 118.692, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.1.8 Security Awareness and Training

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine whether conducting information security awareness training to all individuals interacting with organizations IS contributes in ensuring the confidentiality of information in IS. It was hypothesized that conducting information security awareness training to all individuals interacting with organizations IS contributes to ensuring the confidentiality of information in IS.

Table 4.16 depicts the views when respondents were asked whether all individuals interacting with organizations IS receive information security awareness training. The majority of respondents (61.5%: IT staff) revealed that organizations do not

conduct information security awareness training for all individuals interacting with organizations (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.16). A similar question was asked to management staff on whether organizations conduct security awareness, training and education to employees. The majority of respondents (60%: management staff) revealed that organizations conduct security awareness training and education in ad-hoc (scale 1: unplanned) (Table 4.16); with a median of 0 in SSE-CMM. A similar question was asked to users of IS on whether they receive information security awareness training regularly (annually/twice per year, etc.).

The majority of respondents (64.1%: users of IS) revealed that users of IS do not receive information security awareness training and education (scale 0) (Table 4.16); with a median of 0 in SSE-CMM. Moreover, the Chi-square goodness of fit test results for all three categories (IT staff: $\chi^2(5, N = 39) = 84.231, p < .05$; Management staff: $\chi^2(5, N = 39) = 97.360, p < .05$; IS users: $\chi^2(5, N = 39) = 84.308, p < .05$) in Table 4.16 revealed that conducting information security awareness training to all individuals interacting with organizations contributes to ensuring the confidentiality of information in IS.

The ICT staff revealed that security awareness training and education is not conducted; as opposed to management staff who revealed that it is conducted in ad-hoc (unplanned). This can be due to different security culture perceptions among them, but the difference is small.

Table 4.16: IT Staff Security Awareness and Training

SSE-CMM level	Observed N	Percent
IT staff security awareness and training		
0-Not performed (non-existent)	24	61.5
1-Performed informally (unplanned)	15	38.5
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 84.231, p = .000$, $\sum E_i = \sum O_i = N = 39$		
Management staff: security awareness and training		
0-Not performed (non-existent)	18	36.0
1-Performed informally (unplanned)	30	60.0
2-Partially implemented (planned)	2	4.0
Total	50	100.0
0-Not performed (non-existent)	25	62.5
1-Performed informally (unplanned)	14	35.0
Total	39	97.5

4.2.1.9 Logging, Monitoring and Alertina

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether implementing a process for routinely monitoring logs for detecting unauthorized and anomalous activities and its documentation contributes in ensuring the confidentiality of information in IS. It was hypothesized that implementing a process for routinely monitoring logs for detecting unauthorized and anomalous activities, and its documentation contributes to ensuring the confidentiality of information in IS.

Table 4.17 depicts the views when respondents were asked whether a given organization has a process for routinely monitoring logs to detect unauthorized and anomalous activities and whether it is documented. The findings depicted that, the majority of respondents (64.1%: IT staff) revealed that organizations do monitoring

of logs (scale 1: unplanned) in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.17). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 87.308, p < .05$) in Table 4.17 revealed that implementation of a process for routinely logging, monitoring of logs and alerting contributes in ensuring the confidentiality of information in IS. Thus, ensuring the confidentiality of information, organizations should have a process for routinely logging, monitoring logs and alerting to detect unauthorized and anomalous activities, and it should be documented.

Table 4.17: Logging, Monitoring Logs and Alerting

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	14	35.9
1-Performed informally (unplanned)	25	64.1
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 87.308, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2 Measures for Ensuring the Integrity of Information

This section addresses part of the research question (RQ1): To what extents are the existing security measures ensure confidentiality, integrity and availability of information and information systems? This research question was addressed through a research study to find out the security measures for ensuring the integrity of information during information states in IS, a case study of the education sector in Tanzania. The findings for security measures for ensuring the integrity of information in IS are presented as follows.

4.2.2.1 Access control mechanisms for integrity

Administrative account (super-user) access and operative access to audit logs

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether performing regular reviews of administrative accounts and operative access to audit logs contributes to ensuring the integrity of information in IS. It was hypothesized that performing regular reviews of administrative accounts and operative access to audit logs contributes to ensuring the integrity of information in IS.

Table 4.18 presents the views when respondents were asked whether an organization regularly reviews administrative accounts (account with administrator privileges) and operative access to audit logs. The findings depicted that, the majority of respondents (71.8%: IT staff) revealed that organizations review administrative accounts and operative access to audit logs in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.18). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 100.231, p < .05$) in Table 4.18 revealed that performing regular reviews of administrative accounts and operative access to audit logs contributes in ensuring the integrity of information in IS. Thus, in ensuring the integrity of information, organizations should reviews administrative accounts and operative access to audit logs regularly.

Table 4.18: Review Administrative Accountand Operative Access to Audit Logs

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	11	28.2
1-Performed informally (unplanned)	28	71.8
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 100.231, p = .000$, $\sum E_i = \sum O_i = N = 39$		

Prevent unauthorized access and tempering of system logs

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether the implementation of steps to secure log data to prevent unauthorized access and tampering of systems logs contributes in ensuring the integrity of information in IS. It was hypothesized that the implementation of steps to secure log data to prevent unauthorized access and tampering of systems logs contributes to ensuring the integrity of information in IS.

Table 4.19 presents the views when respondents were asked whether an organization has implemented steps to secure log data to prevent unauthorized access and tampering of systems logs. The findings depicted that, the majority of respondents (82.1%: IT staff) revealed that organizations have implemented steps to secure log data to prevent unauthorized access and tampering of systems logs. in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.19). Moreover, the Chi-square goodness of fit test results ($\chi^2 (5, N = 39) = 123.000, p < .05$) in Table 4.19 revealed that implementation of steps to secure log data to prevent unauthorized access and tampering of systems logs contribute in ensuring the integrity of information in IS. Thus, in ensuring the integrity of

information, organizations should implement steps to secure log data for preventing unauthorized access and tampering of systems logs.

Table 4:19: Prevent Unauthorized Access and Tempering of System Logs

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	5	12.8
1-Performed informally (unplanned)	32	82.1
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 123.000$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.2 Digital Signature

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether encrypting and digitally signing messages (emails) which are sent over an untrusted network (such as the Internet) guarantee that the message sent is the message received (authenticity of information) contributes to ensuring the integrity of information in IS. It was hypothesized that encrypting and digitally signing messages (emails) which are sent over an untrusted network (such as the Internet) guarantee that the message sent is the message received (authenticity of information) contributes in ensuring the integrity of information in IS.

Table 4.20 presents the views when respondents were asked whether messages (emails) sent over an untrusted network (such as the Internet) are encrypted and digitally signed to guarantee that the message sent is the message received (authenticity of information). The findings depicted that, the majority of respondents (100%: IT staff) revealed that messages (emails) are sent without being encrypted and digitally signed over the untrusted network; with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.20). Moreover, the Chi-square goodness of fit test results

($\chi^2(5, N = 39) = 195.000, p < .05$) in Table 4.20 revealed that encrypting and digitally signing messages (emails) which are sent over an untrusted network (such as the Internet) guarantee that the message sent is the message received (authenticity of information) contribute in ensuring integrity of information in IS. Thus, in ensuring the integrity of information, organizations should encrypt and digitally sign messages (e-mails) sent over an untrusted network such Internet.

Table 4.20: Encryption and Digitally Signing Of Messages

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	39	100.0
Median=1.00, E_i per category $= 1/6 * 39 = 6.5$, $\chi^2(df = 5) = 195.000, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.3 Checksum

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether the use of checksum (e.g. MD5, SHA3) to data/information during capturing, processing, storage, and transmission in IS contributes in ensuring the integrity of information in IS. It was hypothesized that the use of checksum (e.g. MD5, SHA3) to data/information during capturing, processing, storage, and transmission in IS contributes to ensuring the integrity of information in IS.

Table 4.21 presents the views when respondents were asked whether a given organization use checksum (e.g. MD5, SHA3) for ensuring the integrity of data/information during processing, storage, and transmission. The findings depicted that, the majority of respondents (66.7%: IT staff) revealed that organisations do not use checksum (e.g. MD5, SHA3) for ensuring the integrity of data/information during capturing, processing, storage, and transmission (scale 0); with a median of 0

in SSE-CMM rating scale of 0-5 (Table 4.21). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 91.000, p < .05$) in Table 4.21 revealed that the use of checksum (e.g. MD5, SHA3) to data/information during capturing, processing, storage, and transmission in IS contribute in ensuring the integrity of information in IS. Thus, in ensuring the integrity of information during capturing, processing, storage, and transmission in IS organizations should use checksum (e.g. MD5, SHA3).

Table 4.21: Checksum

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	26	66.7
1-Performed informally (unplanned)	13	33.3
Total	39	100.0
Median=0.00, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 91.000, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.4 Rotation of Duties Principle

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether the practice of job rotation to breaks up opportunities for collusion and fraudulent activities contributes in ensuring the integrity of information in IS. It was hypothesized that the practice of job rotation to breaks up opportunities for collusion and fraudulent activities contributes to ensuring the integrity of information in IS.

Table 4.22 presents the views when respondents were asked whether a given organization practice job rotation to breaks up opportunities for collusion and fraudulent activities. The findings depicted that, the majority of respondents (64.1%: IT staff) revealed that organizations do not practice job rotation to breaks up

opportunities for collusion and fraudulent activities (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.22). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 79.923, p < .05$) in Table 4.22 revealed that the practice of job rotation to breaks up opportunities for collusion and fraudulent activities contributes in ensuring the integrity of information in IS. Thus, in ensuring the integrity of information, organizations should practice job rotation to breaks up opportunities for collusion and fraudulent activities.

Table 4.22: Job Rotation

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	25	64.1
1-Performed informally (unplanned)	12	30.8
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 79.923, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.5 Segregation of Duties Principle

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether duties are sufficiently segregated (job descriptions issued to all employees and duties well defined) to ensure the detection of unintentional or unauthorized modification of information contributes in ensuring the integrity of information in IS. It was hypothesized that sufficiently segregation of duties (job descriptions issued to all employees and duties well defined) to ensure the detection of unintentional or unauthorized modification of information contributes in ensuring the integrity of information in IS.

Table 4.23 presents the views when respondents were asked whether in given organization duties are sufficiently segregated (job descriptions issued to all employees and duties well defined) to ensure the detection of unintentional or unauthorized modification of information. The findings portrayed that the majority of respondents (69.2%: IT staff) revealed that organizations do segregation of duties in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.23). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 81.769, p < .05$) in Table 4.23 revealed that sufficiently segregation of duties (job descriptions issued to all employees and duties well defined) to ensure the detection of unintentional or unauthorized modification of information contribute in ensuring the integrity of information in IS. Thus, ensuring the integrity of information, duties should be sufficiently segregated in a given organization to ensure the detection of unintentional or unauthorized modification of information.

Table 4.23: Segregation of Duties

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	6	15.4
1-Performed informally (unplanned)	27	69.2
2-Partially implemented (planned)	4	10.3
3-Implementation is in progress (planned and tracked)	2	5.1
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 81.769, p = .000, \sum E_i = \sum O_i = N = 39$		

4.2.2.6 Change Management for Information Systems

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether the implementation of change management for IS (software development/acquisition, change in software, configuration parameters, network,

user interface, etc.); and its changes are documented, communicated, authorized, tested, implemented, monitored and audited contributes in ensuring integrity of information in IS. It was hypothesized that implementation of change management for IS (software development/acquisition, change in software, configuration parameters, network, user interface, etc.); and changes documented, communicated, authorized, tested, implemented, monitored and audited contribute in ensuring the integrity of information in IS.

Table 4.24 presents the views when respondents were asked whether organizations implement change management for IS (software development/acquisition, change in software, configuration parameters, network, user interface, etc.); whether the changes are documented, communicated, authorized, tested, implement, monitored and audited. The findings portrayed that, the majority of respondents (59.0%: IT staff) revealed that organizations implement change management for IS in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.24). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 62.385, p < .05$) in Table 4.24 revealed that implementation of change management for IS (software development/acquisition, change in software, configuration parameters, network, user interface, etc.); and changes documented, communicated, authorized, tested, implemented, monitored and audited contribute in ensuring integrity of information in IS. Thus, for ensuring the integrity of information, organizations should implement change management for IS and the changes should be documented, communicated, authorized, tested, implemented, monitored and audited.

Table 4.24: Change management for information systems

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	9	23.1
1-Performed informally (unplanned)	23	59.0
2-Partially implemented (planned)	7	17.9
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 62.385, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.7 Logging, Monitoring and Alerting

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether automatically logging, monitoring and auditing of security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments contribute in ensuring the integrity of information in IS. It was hypothesized that automatically logging, monitoring and auditing of security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments contributes in ensuring the integrity of information in IS.

Table 4.25 presents the views when respondents were asked whether security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments are automatically logged, monitored and audited. The findings depicted that, the majority of respondents (71.8%: IT staff) revealed that organizations automatically log, monitor and audit security-related activities in ad-hoc (scale 1: unplanned); with a median of

1 in SSE-CMM in Tanzania education sector (Table 4.25). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 94.692, p < .05$) in Table 4.25 revealed that automatically logging, monitoring and auditing of security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments contribute in ensuring the integrity of information in IS. Thus, for ensuring the integrity of information, organizations should automatically log, monitor and audit security-related activities regularly.

Table 4.25: Automatically logging of changes

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	9	23.1
1-Performed informally (unplanned)	28	71.8
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 94.692, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.8 Audit Trail

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether implementing audit trail (audit log) for sensitive IS and periodically monitoring contributes in ensuring the integrity of information in IS. It was hypothesized that implementing an audit trail (audit log) for sensitive data/information in IS and periodically monitoring contributes to ensuring the integrity of information in IS.

Table 4.26 presents the views when respondents were asked whether a given organization has an audit trail (audit log) for sensitive IS and it is periodically monitored. The findings depicted that the majority of respondents (84.6%: IT staff) revealed that organizations implement audit trail for sensitive IS in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.26). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 134.077, p < .05$) in Table 4.26 revealed that implementing audit trail (audit log) for sensitive data/information in IS and periodically monitoring contribute in ensuring the integrity of information in IS. Thus, for ensuring the integrity of information, organizations should implement an audit trail (audit log) for sensitive IS and it should be periodically monitored.

Table 4.26: Audit Logs for Sensitive Information

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	6	15.4
1-Performed informally (unplanned)	33	84.6
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 134.077, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.9 Monitoring LAN, WAN and Wireless Networks

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether continuous monitoring of wired (LAN/WAN) and wireless networks for unauthorized access contribute in ensuring the integrity of information in IS. It was hypothesized that continuous monitoring of wired (LAN/WAN) and wireless networks for unauthorized access contributes to ensuring the integrity of information in IS.

Table 4.27 presents the views when respondents were asked whether a given organization continuously monitor wired (LAN/WAN) and wireless networks for unauthorized access. The findings depicted that, the majority of the respondents (89.7%: IT staff) revealed that organisations monitor their LAN/WAN and wireless networks for unauthorized access in ad-hoc (scale 1: unplanned); with a mean of 0.95, mode of 1 and standard deviation of 0.320 in CMM rating scale of 0-5 (Table 4.27). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 151.000, p < .05$) in Table 4.27 revealed that continuous monitoring of wired (LAN/WAN) and wireless networks for unauthorized access contribute in ensuring the integrity of information in IS. Thus, ensuring the integrity of information, organizations should continuously monitor their LAN/WAN and wireless networks for unauthorized access.

Table 4.27: Monitor Wired (LAN/WAN) And Wireless Networks

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	3	7.7
1-Performed informally (unplanned)	35	89.7
2-Partially implemented (planned)	1	2.6
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 151.000, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.10 Integrity Monitoring Tool

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether integrity monitoring tools for alerting personnel for unauthorized modification of critical system files, configuration files, or content files; and

software configured to perform critical files comparisons at least weekly contributes in ensuring the integrity of information in IS. It was hypothesized that integrity monitoring tools for alerting personnel for unauthorized modification of critical system files, configuration files, or content files; and software configured to perform critical files comparisons at least weekly contributes in ensuring the integrity of information in IS.

Table 4.28 presents the views when respondents were asked whether a given organization has integrity monitoring tools for alerting personnel for unauthorized modification of critical system files, configuration files, or content files; and software configured to perform critical files comparisons at least weekly. The findings portrayed that, the majority of respondents (53.8%: IT staff) revealed that organisations do not have integrity monitoring tools for alerting personnel for unauthorized modification of critical system files, configuration files, or content files (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.28).

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 78.692, p < .05$) in Table 4.28 revealed that integrity monitoring tools for alerting personnel for unauthorized modification of critical system files, configuration files, or content files; and software configured to perform critical files comparisons at least weekly contribute in ensuring integrity of information in IS. Thus, ensuring the integrity of information, organizations should have integrity monitoring tools for alerting personnel for unauthorized modification of critical system files, configuration files, or content files; and software should be configured to perform critical files comparisons at least weekly.

Table 4.28: Integrity monitoring tool

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	21	53.8
1-Performed informally (unplanned)	18	46.2
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 78.692$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.2.11 Least privilege principle/ Need know to the principle

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether procedures for reviewing users' access regularly to ensure only needed privileges are applied and documented contribute in ensuring the integrity of information in IS. It was hypothesized that implementing procedures for reviewing users' access regularly to ensure only needed privileges are applied and documented contributes in ensuring the integrity of information in IS contributes to ensuring the integrity of information in IS.

Table 4.29 presents the views when respondents were asked whether a given organization has procedures for reviewing users' access regularly to ensure only needed privileges are applied and documented. The findings portrayed that, the majority of respondents (64.1%: IT staff) revealed that organizations have implemented procedures for reviewing users' access in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.29). Moreover, the Chi-square goodness of fit test results ($\chi^2 (5, N = 39) = 83.308$, $p < .05$) in Table 4.29 revealed that implementing procedures for reviewing users' access regularly to ensure only needed privileges are applied and documented contribute in ensuring the

integrity of information in IS. Thus, in ensuring the integrity of information, organizations should implement procedures for reviewing users' access regularly, and only needed privileges should be applied and documented.

Table 4.29: Procedures to Review Users' Access

SSE-CMM	Observed N	Percent
0-Not performed (non-existent)	13	33.3
1-Performed informally (unplanned)	25	64.1
2-Partially implemented (planned)	1	2.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 83.308$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3 Measures for Ensuring Availability of Information

This section addresses part of the research question (RQ₁): To what extents are the existing security measures ensure confidentiality, integrity and availability of information and information systems? This research question was addressed through a research study to find out the security measures for ensuring the availability of information during information states (capturing, processing, storage, and transmission) in IS, a case study of the education sector in Tanzania. The findings for security measures for ensuring the availability of information in IS are presented as follows.

4.2.3.1 Business Continuity Plan

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether having a documented business continuity plan for information technology that is based on a business impact analysis, periodically tested, and

reviewed and approved by top management or the board of trustees contributes in ensuring the availability of information in IS. It was hypothesized that having a documented business continuity plan for information technology that is based on a business impact analysis, periodically tested, and reviewed and approved by top management or the board of trustees contributes in ensuring the availability of information in IS contributes in ensuring the integrity of information in IS.

Table 4.30 depicts the view when the respondents were asked whether the given organization has documented business continuity plan for information technology that is based on a business impact analysis, is periodically tested and has been reviewed and approved by top management or the board of trustees. The majority of respondents (51.3%: IT staff) revealed that organizations do not have a business continuity plan (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.30).

The the same question was asked to management staff, the majority of respondents (70%: management staff) revealed that organizations do not have a business continuity plan (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.30). The the same question was asked to users of IS, the majority of respondents (63.2%: users of IS) revealed that organizations do not have a business continuity plan (scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.30).

Moreover, the Chi-square goodness of fit test results for all three categories of respondents (IT staff: $\chi^2(5, N = 39) = 67.615$, $p < .05$; management staff: $\chi^2(5, N = 50) = 124.000$, $p < .05$; users of IS: $\chi^2(5, N = 38) = 124.000$,

$p < .05$) in Table 4.30 revealed that having a documented business continuity plan for information technology that is based on a business impact analysis, periodically tested, and reviewed and approved by top management or the board of trustees contributes in ensuring availability of information in IS. Thus, in ensuring the availability of IS, a given organization should have a documented business plan for information technology that is based on a business impact analysis, periodically tested, and reviewed and approved by top management or the board of trustees.

Table 4.30: Business continuity plan

SSE-CMM level	Observed N	Percent
IT staff: Business continuity planning		
0-Not performed (non-existent)	20	51.3
1-Performed informally (unplanned)	17	43.6
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 67.615$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		
Management staff: Business continuity planning		
0-Not performed (non-existent)	35	70.0
1-Performed informally (unplanned)	15	30.0
Total	50	100.0
Median=0, E_i per category $i=1/6*50=8.3$, $\chi^2 (df = 5) = 124.000$, $p = .000$, $\sum E_i = \sum O_i = N = 50$		
Users of IS: Business continuity planning		
0-Not performed (non-existent)	24	63.2
1-Performed informally (unplanned)	13	34.2
2-Partially implemented (planned)	1	2.6
Total	38	100.0
Median=0, E_i per category $i=1/6*38=6.3$, $\chi^2 (df = 5) = 79.789$, $p = .000$, $\sum E_i = \sum O_i = N = 38$		

4.2.3.2 Incident Management and Response

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine whether incident management and response contribute to ensuring

the availability of information in IS. It was hypothesized that the implementation of incident management and response contributes to ensuring the availability of IS. Table 4.31 presents views when the respondents were asked whether the given organization have incident-handling procedures in place to report and respond to security events throughout the incident lifecycle, including the definition of roles and responsibilities. The majority of respondents (71.8%: IT staff) revealed that organizations have implemented incident-handling procedures in ad-hoc(scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.31).

Further, the findings revealed the views when the management staff was asked (similar question) whether a given organization has an incident response team in place and is functional. The majority of respondents (62%: management staff) revealed that organizations do not have functional incident response team(scale 0); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.31). The findings revealed the views when users of IS were asked (similar question) whether they know where to report information security incidents. The majority of respondents(80%: users of IS) revealed that information security incidents are reported in ad-hoc(scale 1: unplanned), with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.31).

Moreover, the Chi-square goodness of fit test results for all the three categories of respondents (IT staff: ($\chi^2(5, N = 39) = 84.231, p < .05$), management staff: ($\chi^2(5, N = 50) = 108.640, p < .05$), users of IS: ($\chi^2(5, N = 38) = 129.368, p < .05$)) in Table 4.31 revealed that implementation of incident management and response contributes in ensuring availability of IS. Thus, in ensuring the availability

of IS, a given organization should implement incident management and response. This includes incident-handling procedures in place to report and respond to security events throughout the incident lifecycle; incident response team in place and is functional; awareness to users of IS on how; what and where to report information security incidents.

Table 4.31: Incident Management and Response

SSE-CMM level	Observed N	Percent
IT staff: Incident handling procedures and reporting		
0-Not performed (non-existent)	11	28.2
1-Performed informally (unplanned)	26	66.7
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $X^2(df = 5) = 84.231$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		
Management staff: Incident response team		
0-Not performed (non-existent)	31	62.0
1-Performed informally (unplanned)	19	38.0
Total	50	100.0
Median=0, E_i per category $i=1/6*50=8.3$, $X^2(df = 5) = 108.640$, $p = .000$, $\sum E_i = \sum O_i = N = 50$		
Users of IS: Incident reporting		
0-Not performed (non-existent)	6	15.8
1-Performed informally (unplanned)	32	84.2
Total	38	100.0
Median=1, E_i per category $i=1/6*38=6.3$, $X^2(df = 5) = 129.368$, $p = .000$, $\sum E_i = \sum O_i = N = 38$		

4.2.3.3 Awareness of Legal or Compliance Requirements

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether awareness of incident response team to legal or compliance

requirements surrounding evidence collection contributes to ensuring the availability of IS. It was hypothesized that awareness of incident response team to legal or compliance requirements surrounding evidence collection contributes to ensuring the availability of IS.

Table 4.32 presents the views when respondents were asked whether the incident response team is aware of legal or compliance requirements surrounding evidence collection. The majority of respondents (71.8%: IT staff) revealed that incidents response teams are not aware of legal or compliance requirements surrounding evidence collection for information security incidents; with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.32). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 94.692, p < .05$) in Table 4.32 revealed that awareness of incident response team to legal or compliance requirements surrounding evidence collection contributes in ensuring the availability of IS.

Table 4.32: Incident Response Team Aware Of Legal Or Compliance Requirements

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	28	71.8
1-Performed informally (unplanned)	9	23.1
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 94.692, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3.4 Disaster Recovery Plan

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine whether having a disaster recovery plan (DRP) in place contributes

to ensuring the availability of IS. It was hypothesized that having a DRP in place contributes to ensuring the availability of IS.

Table 4.33 reveals the views when respondents were asked whether a given organization has a DRP in place. The majority of respondents (69.2%: IT staff) revealed that organizations have implemented disaster recovery plan in ad-hoc(scale 1: unplanned); with a median of 1 in SSE-CMM with a rating scale of 0-5 (Table 4.33). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 79.923, p < .05$) in Table 4.33 revealed that having a DRP in place contributes to ensuring the availability of IS. Thus, in ensuring the availability of IS a given organization should have a DRP in place.

Table 4.33: Disaster Recovery Plan

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	12	30.8
1-Performed informally (unplanned)	25	64.1
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 79.923, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3.5 Backup Strategies

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether the implementation of backup strategies (normal backups & offsite backups) for data, databases and user files for disaster recovery contributes in ensuring the availability of IS. It was hypothesized that implementation of backup strategies (normal backups & offsite backups) for data, databases and user files for disaster recovery contributes to ensuring the availability of IS.

Table 4.34 presents the views when respondents were asked whether a given organization have implemented backup strategies (normal backups & offsite backups); for data databases and user files for disaster recovery. The majority of respondents (66.7%: IT staff) revealed that organizations have implemented backup strategies in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.34). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 79.923, p < .05$) in Table 4.34 revealed that implementation of backup strategies (normal backups & offsite backups) for data, databases and user files for disaster recovery contributes in ensuring the availability of IS. Thus, in ensuring the availability of IS, a given organization should implement effective backup strategies for recovering from a disaster.

Table 4.34: Backup Strategies

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	4	10.2
1-Performed informally (unplanned)	26	66.7
2-Partially implemented (planned)	9	23.1
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df=5)=79.923, p=.000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3.6 Data Backup Process

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine whether the implementation of the data backup process frequency that is consistency with availability requirements contributes to ensuring the availability of IS. It was hypothesized that the implementation of the data backup process frequency that is consistent with the availability requirements contributes to ensuring the availability of IS.

Table 4.35 presents the views when respondents were asked whether data backup process frequency is consistent with the availability requirements for a given organization. The majority of respondents (66.7%: IT staff) revealed that organizations have ineffective data backup process (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.35). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 84.231, p < .05$) in Table 4.35 revealed that implementation of frequency data backup process that is consistent with availability requirements contributes in ensuring the availability of IS. Thus, in ensuring the availability of IS, organizations should implement data backup process frequently that is consistency with availability requirements.

Table 4.35: Data Backup Process

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	2	5.1
1-Performed informally (unplanned)	26	66.7
2-Partially implemented (planned)	11	28.2
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 84.231, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3.7 Test of Restore Procedures

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether routinely test of restore procedure contributes to ensuring the availability of IS. It was hypothesized that routinely test of restore procedure contributes to ensuring the availability of IS.

Table 4.36 presents the views when respondents were asked whether a given organization routinely test the restore procedure. The majority of respondents (74.4%:

IT staff) revealed that organizations perform testing of the restore procedure in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.36). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 99.308, p < .05$) in Table 4.36 revealed that routinely test of restore procedure contributes to ensuring the availability of IS. Thus, in ensuring the availability of IS, organizations should routinely test the restore procedure.

Table 4.36: Test of Restore Procedures

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	7	17.9
1-Performed informally (unplanned)	29	74.4
2-Partially implemented (planned)	3	7.7
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 99.308, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3.8 Capacity Planning

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to determine whether sufficient capacities (hardware, infrastructure, bandwidth, memory, etc.) to process all requests as quickly as possible contributes in ensuring the availability of IS. It was hypothesized that having sufficient capacities (such as hardware, infrastructure, bandwidth, memory, processor speed) to process all requests as quickly as possible contributes to ensuring the availability of IS. Table 4.37 depicts the views when respondents were asked whether a given organization has sufficient capacities (hardware, infrastructure, bandwidth, memory, etc.) to process all requests as quickly as possible for various IS. The majority of respondents (92.3%: IT staff) revealed that organizations have insufficient capacities

to process all requests as quickly for various IS (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5(Table 4.37).

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 161.154, p < .05$) in Table 4.37 revealed that having sufficient capacities (such as hardware, infrastructure, bandwidth, memory, processor speed) to process all requests as quickly as possible contributes in ensuring the availability of IS. Thus, in ensuring the availability of IS, organizations should have sufficient capacities (such as hardware, infrastructure, bandwidth, memory, processor speed) to process all requests as quickly as possible in IS.

Table 4.37: Sufficient capacities

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	1	2.6
1-Performed informally (unplanned)	36	92.3
3-Implementation is in progress (planned and tracked)	2	5.1
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 161.154, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3.9 Fault Tolerance

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine whether fault tolerance (hardware redundancy, software recovery) contributes to ensuring the availability of IS. It was hypothesized that the implementation of fault tolerance (hardware redundancy, software recovery) contributes to ensuring the availability of IS.

Table 4.38 presents the view when respondents were asked whether IS are implemented with fault tolerance (hardware redundancy, software recovery) to continue with service delivery in case of system failure. The majority of respondents (84.6%: IT staff) revealed that organizations have implemented fault tolerance for IS in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.38). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 132.538, p < .05$) in Table 4.38 revealed that implementation of fault tolerance (hardware redundancy, software recovery) contributes to ensuring the availability of IS. Thus, in ensuring the availability of IS, organizations should implement fault tolerance (hardware redundancy, software recovery) to continue with service delivery in case of systems failure.

Table 4.38: Fault Tolerance

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	5	12.8
1-Performed informally (unplanned)	33	84.6
2-Partially implemented (planned)	1	2.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 132.538, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3.10 Systems Monitoring

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine whether systems monitoring mechanisms contributes to ensuring the availability of IS. It was hypothesized that implementation of systems monitoring mechanisms contributes to ensuring the availability of IS.

Table 4.39 reveals the views when respondents were asked whether a given organization has systems monitoring mechanisms to ensure continuous availability of IS. The majority of respondents (71.8%: IT staff) revealed that organizations have implemented system monitoring mechanisms in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.39). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 94.692, p < .05$) in Table 4.39 revealed that implementation of systems monitoring mechanisms contributes to ensuring the availability of IS. Thus, in ensuring the availability of IS, organizations should implement systems monitoring mechanisms to ensure continuous availability of IS.

Table 4.39: Systems Monitoring Mechanisms

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	9	23.1
1-Performed informally (unplanned)	28	71.8
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 94.692, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.2.3.11 Preventive Measures for Protecting Critical Hardware and Wiring

Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to determine whether having preventative measures for protecting critical hardware and wiring from natural and man-made threats contributes in ensuring the availability of IS. It was hypothesized that the implementation of preventative measures for protecting critical hardware and wiring from natural and man-made threats contributes to ensuring the availability of IS.

Table 4.40 depicts the views when respondents were asked whether a given organization has preventative measures in place to protect critical hardware and wiring from natural and man-made threats. The majority of respondents (82.1%: IT staff) revealed that organizations have implemented preventative measures to protect critical hardware and wiring from natural and man-made threats in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.40). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 124.231$, $p < .05$) in Table 4.40 revealed implementation of preventative measures for protecting critical hardware and wiring from natural and man-made threats contributes in ensuring the availability of IS. Thus, in ensuring the availability of IS, organizations should implement preventative measures to protect critical hardware and wiring from natural and man-made threats.

Table 4.40: Preventative Measures to Protect Critical Hardware and Wiring

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	6	15.4
1-Performed informally (unplanned)	32	82.1
2-Partially implemented (planned)	1	2.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 124.231$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.3 Security Controls and Security Domains

This presents the research findings regarding security controls for ensuring the security of information during capturing, processing, storage, and transmission in IS. It addresses the research question, RQ₂: To what extents are the existing security controls to ensure the security of information and information systems? The security controls were grouped into 15 domains namely: information security policy,

organisational of information security, human resources security, asset management, access control, cryptography, physical and environmental security, operations security, communication security, systems acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, compliance, and risk management.

The data were collected using a survey questionnaire (Appendix B), semi-structured interview (Appendix B) and document review. The survey data were cleaned, coded, entered into the analysis database (Appendix BI) and analyzed using R statistical computing packages. Non-parametric Chi-square goodness fit test was carried out to test for a significant contribution of the findings of the results. The assessment was based on SSE-CMM with a rating scale of 0-5. The analysis was performed based on the IT security domain. Furthermore, data collected through a semi-structured interview and document review was cleaned, coded and analyzed. The results findings are presented as follows.

4.3.1 Security Policy

This section presents the finding of institution maturity level on information security policy implementation. This assesses how an institution expresses its intent with regard to information security. Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the effectiveness of security policy. It was hypothesized that effective implementation of security policy controls contributes to enhancing the security of IS. These information security policy controls include information security policy that has been approved by management; information

security policy been published and communicated to all relevant parties; review the information security policy at defined intervals to encompass significant change and monitor for compliance. Results findings for assessed security controls for security policy are summarized in Table 4.41. Moreover, the detailed findings for security controls for information security policy have been presented in the following paragraphs.

Table 4.41: Summary Results for Information Security Policy Controls

S/N	Security controls	Results
i	The information security policy that has been approved by management	Majority of respondents (more than 54%) revealed that it has been approved in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating of 0-5; Chi-square goodness of fit test with $p < .05$.
ii	Information security policy has been published and communicated to all relevant parties	Majority of respondents (more than 68%) revealed that it has not been published and communicated to all employees/relevant stakeholders (scale 0: non-existent); with a median of 0 in SSE-CMM rating of 0-5; Chi-square goodness of fit test with $p < .05$.
iii	Review the information security policy at defined intervals to encompass significant change and monitor for compliance	Majority of respondents (more than 94%) revealed that organizations do not review their information security policies (scale 0: non-existent); with a median of 0 in SSE-CMM rating of 0-5; Chi-square goodness of fit test with $p < .05$.

Approval of information security policy

Table 4.42 depicts the view when the respondents were asked whether a given organization has an information security policy that has been approved by the top management/board of directors. The majority of respondents (54%: Management staff) revealed that information security policy in most of the organizations in the education sector in Tanzania has been approved in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.42).

The the same question was asked to IT staff, the majority of respondents (51.3%: IT staff) revealed that organizations have information security policy which has been approved in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.42). The the same question was asked to users of IS, the majority of respondents (56.4%: users of IS) revealed that organizations have information security policy which has been approved in ad-hoc (scale 1:unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.42).

Moreover, the Chi-square goodness of fit test results for all three categories of respondents (management staff: $\chi^2(5, N = 50) = 86.080$, $p < .05$; IT staff: $\chi^2(5, N = 39) = 50.385$; $p < .05$, users of IS: $\chi^2(5, N = 39) = 67.000$, $p < .05$) in Table 4.42 revealed that effective implementation of security policy controls (such as review the information security policy at defined intervals to encompass significant change and monitor for compliance) contributes to enhancement of security for IS. Thus, for enhancing the security of IS, organizations should have an information security policy which has been approved by top management.

Table 4.42: Information Security Policy Approved

SSE-CMM level	Observed N	Percent
Management staff: Information Security Policy approved		
0-Not performed (non-existent)	20	40.0
1-Performed informally (unplanned)	27	54.0
2-Partially implemented (planned)	2	4.0
3-Implementation is in progress (planned and tracked)	1	2.0
Total	50	100.0
Median=1, E_i per category $i=1/6*50=8.3$, $\chi^2(df = 5) = 86.080$, $p = .000$, $\sum E_i = \sum O_i = N = 50$		
IT staff: Information Security Policy approved		

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	12	30.8
1-Performed informally (unplanned)	20	51.3
2-Partially implemented (planned)	6	15.4
3-Implementation is in progress (planned and tracked)	1	2.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 50.385, p = .000$, $\sum E_i = \sum O_i = N = 39$		
Users of IS: Information Security Policy approved		
0-Not performed (non-existent)	14	35.9
1-Performed informally (unplanned)	22	56.4
2-Partially implemented (planned)	3	7.7
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 67.000, p = .000$, $\sum E_i = \sum O_i = N = 39$		

Publishing and communicating information security policy to relevant parties

Table 4.43 depicts the view when the respondents were asked whether information security policy has been published and communicated to all employees and relevant stakeholders. The majority of respondents (68%: Management staff) revealed that information security policy has not been published and communicated to all employees/relevant stakeholders (scale 0:non-existent); with a median of 0 in SSE-CMM rating scale of 0-5(Table 4.43). The same question was asked of IT, staff, the majority of respondents (71.8%: IT staff) revealed that information security policy has not been published and communicated to all employees/relevant stakeholders (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 (Table 4.43). The same question was asked to users of IS, the majority of respondents (71.8% of respondents: users of IS) revealed that information security policy has not been published and communicated to all employees/relevant stakeholders (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 (Table 4.43).

Table 4.43: Information Security Policy Published and Communicated

SSE-CMM level	Observed N	Percent
Management staff: Information Security Policy published and communicated		
0-Not performed (non-existent)	34	68.0
1-Performed informally (unplanned)	15	30.0
2-Partially implemented (planned)	1	2.0
Total	50	100.0
Median=0, E_i per category $i=1/6*50=8.3$, $\chi^2 (df = 5) = 115.840$, $p = .000$, $\sum E_i = \sum O_i = N = 50$		
IT staff: Information Security Policy published and communicated		
0-Not performed (non-existent)	28	71.8
1-Performed informally (unplanned)	10	25.6
3-Implementation is in progress (planned and tracked)	1	2.6
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 97.154$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		
Users of IS: Information Security Policy reading		
0-Not performed (non-existent)	28	71.8
1-Performed informally (unplanned)	10	25.6
2-Partially implemented (planned)	1	2.6
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 97.154$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

Moreover, the Chi-square goodness of fit test results for all three categories of respondents (management staff: $\chi^2 (5, N = 50) = 86.080$, $p < .05$; IT staff: $\chi^2 (5, N = 39) = 97.154$; $p < .05$, users of IS: $\chi^2 (5, N = 39) = 97.154$, $p < .05$) in Table 4.43 revealed that effective implementation of security policy controls (such as publishing and communicating information security policy to all employees/relevant stakeholders) contributes to enhancement of security for IS. This study portrayed that most of the information security policies which have been approved have not been operationalized (left in file cabinets). Thus, for enhancing the security of IS, organizations should ensure that information security policies are published and communicated to employees/relevant stakeholders.

Review of information security policy

Table 4.44 depicts the view when the respondents were asked whether a given organization review information security policy at defined intervals (every 1 year, 2 years, etc.) to encompass significant change and monitor compliance. The majority of respondents (96%: Management staff) revealed that organizations do not review their information security policies regularly (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 (Table 4.44). The same question was asked of IT staff, the majority of respondents (94.9%: IT staff) revealed organizations do not review their information security policies regularly (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 (Table 4.44).

The same question was asked to users of IS, the majority of respondents (100%: users of IS) revealed that organizations do not review their information security policies regularly (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 (Table 4.44). This study portrayed that information security policies are not reviewed regularly (left in file cabinets). Moreover, the Chi-square goodness of fit test results for all three categories of respondents (management staff: $\chi^2(5, N = 50) = 226, p < .05$; IT staff: $\chi^2(5, N = 39) = 171.923, p < .05$, users of IS: $\chi^2(5, N = 39) = 97.154, p < .05$) in Table 4.44 revealed that effective implementation of security policy controls (such as review of information security policy) contributes to enhancing of security for IS. Thus, for enhancing the security of IS, organizations should review their information security policies regularly.

Table 4.44: Information security policy reviewed

SSE-CMM level	Observed N	Percent
Management staff: Information Security Policy approved		
0-Not performed (non-existent)	48	96.0
1-Performed informally (unplanned)	2	4.0
Total	50	100.0
Median=0, E_i per category $i=1/6*50=8.3$, $\chi^2 (df = 5) = 226.960$, $p = .000$, $\sum E_i = \sum O_i = N = 50$		
IT staff: information security policy reviewed		
0-Not performed (non-existent)	37	94.9
1-Performed informally (unplanned)	1	2.6
3-Implementation is in progress (planned and tracked)	1	2.6
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 171.923$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		
Users of IS: information security policy reviewed		
0-Not performed (non-existent)	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 195.000$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.3.2 Organisational of Information Security

This section presents an assessment of the organization of information security controls based on SSE-CMM. This assesses how an organization manages its information security across the entire enterprise, including how the leadership commits its support and provides overall direction. Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to assess the organization of information security controls during information state (capturing, processing, storage, and transmission) in Tanzania education sector. It was hypothesized that effective implementation of organization information security controls contributes to enhancing the security of IS. Results findings for assessed organizational of information security for security policy are summarized in Table 4.45. Moreover, the

detailed findings for security controls for organizational information security have been presented in the following paragraphs.

Table 4.45: Summary results for organizational information security

S/N	Security controls	Results
i	The organization has an individual with enterprise-wide information security responsibility and authority written in their job description.	The majority of respondents (51%: management staff) revealed that organizations do not have staff assigned security responsibilities (scale 0: non-existent) median of 0 with a median of 1 in SSE-CMM rating 0-5; Chi-square goodness of fit test, $\chi^2=92.429$ with $p<.05$.
ii	The organization has an information security committee in place and is functional.	The majority of respondents (more than 57%) revealed that organizations do not have information security committee in place which is functional (scale 0: non-existent); with a median of 0 in SSE-CMM 0-5 rating scale; Chi-square goodness of fit test, $\chi^2 = 87.286$ with $p<.05$.
iii	Employees sign terms and conditions that include responsibilities for information security.	The majority of respondents (more than 59%) revealed that employees do not sign terms and conditions that include responsibilities for information security (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5; Chi-square goodness of fit test, $\chi^2 = 66.077$ with $p<.05$.
iv	Budget allocation for an information security program	The majority of respondents (more than 71%) revealed that organizations do not have a budget allocation for information security program (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5; Chi-square goodness of fit test, $\chi^2 = 121.815$ with $p<.05$.
v	Organization specifies security requirements in contracts with external entities (third party) before granting access to sensitive information assets.	Most organizations (more than 57%) revealed that organizations specify security requirements in contracts in an ad-hoc manner with external entities before granting access to sensitive information assets; with a median of 1 in SSE-CMM rating scale 0-5.
vi	Users of IS sign confidential or non-disclosure agreement for the protection of an organization's information assets.	The majority of respondents (more than 66%) revealed that employees do not sign confidentiality or non-disclosure agreement for the protection of organizations' information assets (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5.

Organization security responsibility defined and assigned

Table 4.46 depicts the view when the respondents were asked whether organizations have staff assigned security responsibility and report to top management. The majority of respondents (51%: management staff) revealed that organizations do not have staff assigned security responsibilities (scale 0: non-existent) median of 0 (Table 4.46).

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 49) = 92.429$, $p < .05$) in Table 4.46 revealed that having a staff assigned security responsibility, and who report to top management contributes in enhancing the availability of IS. Thus, for enhancing the security of IS organizations should have staff assigned security responsibilities.

Table 4.46: Security Responsibility

	SSE-CMM level	Observed N	Percent
	0-Not performed (non-existent)	25	51.0
	1-Performed informally (unplanned)	23	46.9
	2-Partially implemented (planned)	1	2.0
	Total	49	100.0

Median=1, E_i per category $i = 1/6 * 49 = 8.2$,
 $\chi^2(df = 5) = 92.429$, $p = .000$,
 $\sum E_i = \sum O_i = N = 49$

Information security committee

Table 4.47 depicts the view when the respondents were asked whether a given organization has information security committee in place, and is functional. The majority of respondents (57.1%: management staff) revealed that organizations do not have information security committee in place which is functional (scale 0: non-existent); with a median of 0 in SSE-CMM 0-5 rating scale (Table 4.47).

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 49) = 87.286$, $p < .05$) in Table 4.47 revealed that having a functional information security committee in place contributes to enhancing the availability of IS. Thus, for enhancing the security of IS organizations should have information security committee in place, and it should be functional.

Table 4.47: Information Security Committee

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	28	57.1
1-Performed informally (unplanned)	18	36.7
2-Partially implemented (planned)	2	4.1
3-Implementation is in progress (planned and tracked)	1	2.0
Total	49	100.0

Median=1, E_i per category $i=1/6*49=8.2$,
 $\chi^2(df = 5) = 87.286$, $p = .000$,
 $\sum E_i = \sum O_i = N = 49$

Terms and conditions: responsibilities for information security

Table 4.48 depicts the views when the respondents were asked whether employees sign terms and conditions that include responsibilities for information security. The majority of respondents (59%: users of IS) revealed that employees do not sign terms and conditions that include responsibilities for information security (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 in the education sector in Tanzania (Table 4.48).

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 66.077$, $p = .000$, $p < .05$) in Table 4.48 revealed that employees should sign terms and conditions that include responsibilities for information security. Thus, for enhancing the security of IS employees should sign terms and conditions that include responsibilities for information security.

Table 4.48: Signing Terms and Conditions: Responsibilities for Security

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	23	59.0
1-Performed informally (unplanned)	12	30.8
2-Partially implemented (planned)	3	7.7
4-Fully implemented (well defined and auditable)	1	2.6
Total	39	100.0

<p>Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 66.077$, $p = .000$, $\sum E_i = \sum O_i = N = 39$</p>
--

Budget allocation for the information security program

Table 4.49 depicts the view when the respondents were asked whether a given organization do the budget allocation for an information security program. The majority of respondents (71.4%: Management staff) revealed that organizations do not have a budget allocation for information security program (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 (Table 4.49). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 49) = 121.815$, $p < .05$) in Table 4.49 revealed that budget allocation for the information security program contributes to enhancing the security of IS. Thus, for enhancing the security of IS organizations should have a budget allocation for the information security program.

Table 4.49: Budget: information security program

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	35	71.4
1-Performed informally (unplanned)	13	26.5
2-Partially implemented (planned)	1	2.0
Total	49	100.0
<p>Median=1, E_i per category $i=1/6*49=8.2$, $\chi^2(df = 5) = 121.815$, $p = .000$, $\sum E_i = \sum O_i = N = 49$</p>		

Sign confidential or non-disclosure agreement

Table 4.50 depicts the view when the respondents were asked whether employees sign a confidential or non-disclosure agreement for the protection of an organisation's information assets. The majority of respondents (66.7%: users of IS) revealed that employees have not signed confidential or non-disclosure agreement

for the protection of organization's information assets (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 (Table 4.50). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 78.385$, $p < .05$) in Table 4.50 revealed that employees should sign confidentiality or non-disclosure agreement for the protection of an organization's information assets. Thus, for enhancing the security of IS employees should sign a confidential or non-disclosure agreement for the protection of an organisation's information assets.

Table 4.50: Signing Confidential or Non-Disclosure Agreement

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	26	66.7
1-Performed informally (unplanned)	9	23.1
2-Partially implemented (planned)	1	2.6
3-Implementation is in progress (planned and tracked)	1	2.6
4-Fully implemented (well defined and auditable)	2	5.1
Total	39	100.0
Median=1, E_i per category $i = 1/6 * 39 = 6.5$, $\chi^2(df = 5) = 78.385$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.3.3 Human Resources Security

This section presents an assessment of human resources security controls. This assesses an organization's safeguards and processes for ensuring that all employees (including contractors and any user of sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated. Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the human resources security controls. It was hypothesized that effective implementation of human resources security controls contributes to enhancing the security of IS. Results findings for assessed human resources security controls are summarized in Table 4.51.

Furthermore, the detailed findings for security controls for human resources security have been presented in the following paragraphs.

Table 4.51: Summary Results for Human Resources Security

S/N	Security controls	Results
i	Screening/ background checks (vetting)	Majority of respondents (more than 56%) revealed that organizations perform screening, background checks (vetting); with a median of 4 in SSE-CMM rating scale 0-5; with Chi-square goodness of fit test, $\chi^2 = 13.512, p < .05$.
ii	Security awareness training and education to users of IS	The majority of respondents (more than 56%) revealed that organizations conduct security awareness, training and education to employees in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale 0-5; with Chi-square goodness of fit test, $\chi^2 = 87.308, p < .05$.
iii	Specialized role-based training to employees	The findings revealed that most organizations do not conduct specialized role-based training to employees; with a median of 0 in the SSE-CMM rating scale of 0-5.
iv	Information security programs	The findings revealed that most institutions do not have information security programs that clearly state responsibilities, liabilities, and consequences; with a median of 0 in the SSE-CMM rating scale of 0-5
v	Revoking system access, building access and returning assigned assets on termination and change of employment	The findings revealed that most organizations have an ad-hoc (unplanned) process for revoking system access, building access and returning assigned assets on termination; with a median of 1 in SSE-CMM rating scale of 0-5.
vi	Revoking system access when there is a position change or when responsibilities change	The findings revealed that most institutions have an ad-hoc (unplanned) process for revoking system access when there is a position change or when responsibilities change; with a median of 1 in SSE-CMM rating scale of 0-5.
vii	Disciplinary action is taken against the non-compliant employee to information security policy	The majority of respondents (more than 84%) revealed that disciplinary action is not taken against the non-compliant employee(s) to information security policy (scale 0: non-existent) or it is done in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale 0-5; Chi-square goodness of fit test results ($\chi^2 = 48.846, p < .05$).

Screening/ background checks (vetting)

Table 4.52 depicts the view when the respondents were asked whether a given organization perform screening/ background checks (vetting) of employees. The majority of respondents (78%: management staff) revealed that organizations perform screening/ background checks (vetting) (scale 4-5: Fully implemented, monitored and auditable); with a median of 4 in SSE-CMM (Table 4.52). The same

question was asked to IT staff, the majority of respondents (56.4%: IT staff) revealed that organizations perform screening/ background checks (vetting) (scale 4-5: Fully implemented, monitored and auditable); with a median of 4 in SSE-CMM rating scale 0-5 (Table 4.52).

Moreover, the Chi-square goodness of fit test results for management and IT staff respondents (management staff: $\chi^2(5, N = 50) = 48.640$, $p < .05$; IT staff: $\chi^2(5, N = 39) = 13.152$; $p < .05$) in Table 4.52 revealed that performing screening/ background checks (vetting) contributes to the enhancement of security for IS. This study portrayed that organizations in the education sector in Tanzania perform screening/ background checks (vetting); this result is supported by the fact that it is mandatory in Government institutions to perform vetting of employees, and is overseen by Government general security officer. Thus, for enhancing the security of IS organizations should perform the vetting of employees and suppliers/vendors from time to time.

Table 4.52: Screening, Background Checks

SSE-CMM level	Observed N	Percent
Management staff: Screening/background checks		
1-Performed informally (unplanned)	3	6.0
2-Partially implemented (planned)	2	4.0
3-Implementation is in progress (planned and tracked)	6	12.0
4-Fully implemented (well defined and auditable)	22	44.0
5-Fully implemented and regularly updated (monitored and audited for compliance)	17	34.0
Total	50	100.0
Median=1, E_i per category $i=1/6*50=8.3$, $\chi^2(df = 5) = 48.640$, $p = .000$, $\sum E_i = \sum O_i = N = 50$		
IT staff: Screening/background checks		
0-Not performed (non-existent)	3	7.7

SSE-CMM level	Observed N	Percent
1-Performed informally (unplanned)	1	2.6
2-Partially implemented (planned)	7	17.9
3-Implementation is in progress (planned and tracked)	6	15.4
4-Fully implemented (well defined and auditable)	12	30.8
5-Fully implemented and regularly updated (monitored and audited for compliance)	10	25.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 13.152, p = .022$, $\sum E_i = \sum O_i = N = 39$		

Security awareness, training, and education

Table 4.53 depicts the view when the respondents were asked whether a given organization conduct security awareness, training, and education to employees. The majority of respondents (60 %: management staff) revealed that organizations conduct security awareness, training and education to employees in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.53).

The same question was asked to IT-staff, the majority of respondents (56.4%: IT staff) revealed that organizations should conduct security awareness, training and education to employees in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.53). The same question was asked to users of IS, the majority of respondents (64.1%: users of IS) revealed that organizations do not conduct security awareness, training, and education to employees (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale 0-5 (Table 4.53).

Table 4.53: Security Awareness, Training, and Education

SSE-CMM level	Observed N	Percent
Management staff: Security awareness, training, and education		
0-Not performed (non-existent)	18	36.0
1-Performed informally (unplanned)	30	60.0
2-Partially implemented (planned)	2	4.0
Total	50	100.0
Median=1, E_i per category $i=1/6*50=8.3$, $\chi^2(df = 5) = 97.360$, $p = .000$, $\sum E_i = \sum O_i = N = 50$		
IT staff: Security awareness, training, and education		
0-Not performed (non-existent)	17	43.6
1-Performed informally (unplanned)	22	56.4
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 97.360$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		
Users of IS: Security awareness, training, and education		
0-Not performed (non-existent)	25	64.1
1-Performed informally (unplanned)	14	35.9
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 87.308$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

This study portrayed that security awareness, training and education to employees either not conducted or done in an ad-hoc manner. Moreover, the Chi-square goodness of fit test results for all three categories of respondents (management staff: $\chi^2(5, N = 50) = 97.360$, $p < .05$; IT staff: $\chi^2(5, N = 39) = 79.923$; $p < .05$, users of IS: $\chi^2(5, N = 39) = 87.308$, $p < .05$) in Table 4.53 revealed that security awareness, training, and education to employees contribute to the enhancement of security for IS.

Likewise, Table 4.54 presents findings on whether all individuals interacting with organizations receive information security awareness training (qn11); based on a

semi-structured interview with 18 subject matter experts (Head of ICT, IT staff) in seven organizations under study. The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that individuals interacting with organizationsø IS do not receive information security awareness training; with a median of 0 in the SSE-CMM rating scale of 0-5 (Table 4.54). Thus, for enhancing the security of IS, organizations should conduct security awareness, training, and education to employees regularly.

Table 4.54: Security awareness training

Security controls	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Security awareness training (qn11)	0	0	1	0	0	1	1	0
Respondents : Head of ICT & IT staff	2	1	1	4	3	3	4	18

Specialized role-based training to employees

Table 4.55 presents findings on whether organizations conduct specialized role-based training to employees (qn12). This was based on a semi-structured interview with 18 subject matter experts (Head of ICT, IT staff) in seven organizations under study. The semi-structured interview was conducted in each of the seven organizations under study using an interview data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations do not conduct specialized role-based training to employees; with a median of 0 in the SSE-CMM rating scale of 0-5 (Table 4.55). Thus, for enhancing the security of IS, organizations should conduct specialized role-based training for employees.

Table 4.55: Specialized Role-Based Training

Security controls	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Specialized role-based training (qn12)	0	0	1	0	0	1	1	0
Respondents : Head of ICT & IT staff	2	1	1	4	3	3	4	18

Information security programs

Table 4.56 presents findings on whether organizations have information security programs that clearly state responsibilities, liabilities, and consequences (qn13). This was based on a semi-structured interview with 18 subject matter experts (Head of ICT, IT staff) in seven organizations under study (Table 4.56). The semi-structured interview was conducted in each of the seven organizations under study using an interview data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most institutions do not have information security programs that clearly state responsibilities, liabilities, and consequences; with a median of 0 in the SSE-CMM rating scale of 0-5 (Table 4.56). Thus, for enhancing the security of IS, organizations should have information security programs that clearly state responsibilities, liabilities, and consequences.

Table 4.56: Information security programs

Security controls	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Information security programs (qn13)	0	0	0	0	0	0	0	0
Respondents : Head of ICT & IT staff	2	1	1	4	3	3	4	18

Revoking system access and returning assigned assets on termination

Table 4.57 presents findings on whether organizations have a process for revoking system access, building access and returning assigned assets on termination and change of employment (qn14). This was based on a semi-structured interview with 18 subject matter experts (Head of ICT, IT staff) in seven organizations under study (Table 4.57). The semi-structured interview was conducted in each of the seven organizations under study using an interview data collection matrix tool (Appendix

B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have implemented a process for revoking system access, building access and returning assigned assets on termination and change of employment in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS, organizations should have a process for revoking system access, building access and returning assigned assets on termination and change of employment.

Table 4.57: Revoking System Access on Termination

Security control	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Revoking system access and returning assigned assets on termination (qn14)	1	1	1	1	1	1	1	1
Respondents : Head of ICT &IT Staff	2	1	1	4	3	3	4	18

Revoking system access when there are a position change or responsibilities

Table 4.58 presents findings on whether organizations have a process for revoking system access when there is a position change or when responsibilities change (qn15). This was based on a semi-structured interview with 18 subject matter experts (Head of ICT, IT staff) in seven organizations under study (Table 4.58). The semi-structured interview was conducted in each of the seven organizations under study using an interview data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most institutions have implemented a process for revoking system access when there is a position change or when responsibilities change in an ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.58). Thus, for enhancing the security of IS, organizations should have a process for

revoking system access when there is a position change or when responsibilities change.

Table 4.58: Revoking system access when there are a change of roles

Security Domain	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Revoking system access when there is a position change or when responsibilities change (qn15).	1	1	1	1	1	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Disciplinary action was taken against the non-compliant

Table 4.59 depicts the view when the respondents were asked whether disciplinary action is taken against the non-compliant employee to information security policy. The majority of respondents (84.6 %: users of IS) revealed that disciplinary action is not taken against the non-compliant employee(s) to information security policy (scale 0: non-existent) or it is done in ad-hoc (Scale 1: unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.59). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 48.846, p < .05$) in Table 4.59 revealed that disciplinary action should be taken against the non-compliant employee(s) to security policy. Thus, for enhancing the security of IS, disciplinary action should be taken against the non-compliant employee(s) to information security policy.

Table 4.59: Disciplinary Action: Non-Compliant With Information Security Policy

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	14	35.9
1-Performed informally (unplanned)	19	48.7
2-Partially implemented (planned)	3	7.7
3-Implementation is in progress (planned and tracked)	2	5.1
4-Fully implemented (well defined and auditable)	1	2.6
Total	39	100.0

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	14	35.9
1-Performed informally (unplanned)	19	48.7
2-Partially implemented (planned)	3	7.7
3-Implementation is in progress (planned and tracked)	2	5.1
4-Fully implemented (well defined and auditable)	1	2.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 48.846$, $p = .000$		
$\sum E_i = \sum O_i = N = 39$		

4.3.4 Asset Management

This assesses the existing security controls for asset management. Asset management involves identification, tracking, classifying, and assigning ownership for the most important information resources (assets) to ensure they are adequately protected. Both quantitative and qualitative data were collected. The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B).

The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the asset management controls. It was hypothesized that effective implementation of asset management controls contributes to enhancing the security of IS. Results findings for assessed asset management controls are summarized in Table 4.60. Furthermore, the detailed findings for security controls for asset management have been presented in the following paragraphs.

Table 4.60: Summary results for asset management

S/N	Security controls	Results
i	Identification of critical information assets	The findings revealed that most organizations identify critical information assets in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5
ii	Classify information resources (assets) to indicate the appropriate access levels of information security.	The majority of respondents (79.5 %: IT staff) revealed that organizations have classified its information resources (assets) by indicating access levels (public, confidential, secret) and it has documented them in ad-hoc manner (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale 0-5; with Chi-square goodness of fit test results, $\chi^2(5, N = 39) = 118.692, p < .05$.

Identification of critical information assets

Table 4.61 presents findings on whether organizations identify critical information assets and the functions that rely on them (qn9). This was based on a semi-structured interview with 18 subject matter experts (Head of ICT, IT staff) in seven organizations under study (Table 4.61). The semi-structured interview was conducted in each of the seven organizations under study using an interview data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations identify critical information assets in ad-hoc; with a median of 1 in SSE-CMM rating scale of 0-5 in Tanzania education sector.

Table 4.61: Identification of Critical Information Assets

Security controls	Organisation							Median/Total
	L	K	O	M	P	N	Q	
Identification of critical information assets and the functions that rely on them (qn9)	1	0	1	0	0	1	1	1
Respondents : Head of ICT & II Staff	2	1	1	4	3	3	4	18

Classification of information resources (assets) by indicating access levels

Table 4.62 depicts the view when the respondents were asked whether a given organization has classified its information resources (assets) by indicating access levels (public, confidential, secret) and it has documented them? The majority of respondents (79.5 %: IT staff) revealed that organizations have classified its information resources (assets) by indicating access levels (public, confidential, secret) and it has documented them in ad-hoc manner (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.62). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 118.692$, $p < .05$) in Table 4.62 revealed that organizations should classify and document its information resources (assets) by indicating access levels (public, confidential, secret). Thus, for enhancing the security of IS, the organisation should classify and document its information resources (assets) by indicating access levels (public, confidential, secret).

Table 4.62: Classifying information resources - assets

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	8	20.5
1-Performed informally (unplanned)	31	79.5
Total	39	100.0
Median=1, E_i per category $i=1/6*50=8.3$, $\chi^2(df = 5) = 48.640$, $p = .000$, $\sum E_i = \sum O_i = N = 50$		

Thus, the study depicted that assets management is performed in ad-hoc (unplanned); it is questionable to ensure adequate protection of information assets without classifying them into appropriate information security levels. For enhancing the security of IS, organizations should identify and classify information assets into appropriate information security levels such as top secret, secret, and the public.

4.3.5 Access Control

This assesses the existing security controls for access control. This assesses an organization use of administrative, physical or technical security features to manage how users and systems communicate and interact with other information resources. Both quantitative and qualitative data were collected. The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B).

The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the security controls for access control. It was hypothesized that effective implementation of security controls for access control contributes to enhancing the security of IS. Results findings for security controls for access control are summarized in Table 4.63. Furthermore, the detailed findings for security controls for access control have been presented in the following paragraphs.

Table 4.63: Summary Results for Access Controls

S/N	Security controls	Results
i	Access control policy	Majority of respondents (82.1%: IT staff) revealed that organizations have implemented access control policy in an ad-hoc manner with a median of 1 in SSE-CMM scale of 0-5. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 123.000$, $p < .05$) revealed that organizations should implement an access policy for IS.
ii	Rules (policy) for using information systems	Majority of respondents (82.1%: users of IS) revealed that organizations have implemented rules (policy) for using IS in an ad-hoc manner (scale 1: unplanned); with a median of 1. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 124.231$, $p < .05$) revealed that organizations should implement rules (policy) for using IS.
iii	Access control policy for authorizing and revoking access rights	Findings revealed that most organizations have implemented access control policy for authorizing and revoking access rights to IS in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5.
iv	Process for granting and revoking appropriate user access	Findings revealed that most organizations have an ad-hoc (unplanned) process for granting and revoking appropriate user access; with a median of 1 in SSE-CMM rating scale of 0-5
v	Password management program that follows current security standards	Findings revealed most organizations do not have a password management program that follows current security standards; with a median of 0 in the SSE-CMM rating scale of 0-5
vi	Procedures for reviewing access regularly	Findings revealed that most organizations do not have procedures for reviewing users' access; with a median of 0 in the SSE-CMM rating scale of 0-5.
vii	Securing remote access	Findings revealed that most organizations have implemented controls for securing remote access services in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5.
viii	Prevent and detect rogue access to LAN	The findings revealed that most organizations have not implemented specific controls for preventing and detecting rogue access to wireless LANs; with a median of 0 in the SSE-CMM rating scale of 0-5
ix	Block or restrict unencrypted sensitive information to untrusted networks	Findings revealed that most organizations have not employed technologies to block or restrict unencrypted sensitive information from travelling to untrusted networks; with a median of 0 in the SSE-CMM rating scale of 0-5
x	Restrict the sharing of passwords	Findings revealed that most organizations do not have a policy for restricting the sharing of passwords; with a median of 0 in the SSE-CMM rating scale of 0-5.
xi	Authorization system to enforces time limits lockout on login failure and limits minimum privileges defaults	Findings revealed that most organizations have implemented authorization system for enforcing time limits lockout on login failure and which defaults to minimum privilege in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5.
xii	Policies and controls for the use of mobile devices	Findings revealed that most organizations have not implemented policies and controls for the use of mobile devices; with a median of 0 in the SSE-CMM rating scale of 0-5.
xiii	Encryption of mobile computing devices (i.e., laptops, tablets, etc.)	Findings revealed that most organizations do not employ encryption on mobile computing devices; with a median of 0 in the SSE-CMM rating scale of 0-5.
xiv	Telework policy that addresses multifactor access and endpoint security	Findings revealed that most organizations do not have telework policy for addressing multifactor access and security requirements for the endpoint used; with a median of 0 in SSE-CMM rating scale of 0-5.

Access control policy

Table 4.64 depicts the views when the respondents were asked whether organizations have access control policy for accessing IS resources (databases, file servers, mail server, internet, LAN). The majority of respondents (82.1%: IT staff) revealed that organizations have implemented access control policy for accessing IS resources in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.64). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 123.000$, $p < .05$) in Table 4.64 revealed that organizations should implement rules (policy) for using IS (e-mail, the Internet, file-server, applications, LAN). Thus, for enhancing the security of IS organizations should implement an access control policy for accessing IS resources.

Table 4.64: Access control policy

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	5	12.8
1-Performed informally (unplanned)	32	82.1
2-Partially implemented (planned)	2	5.1
Total	39	100.0
Median=1, E_i per category $i = 1/6 * 39 = 6.5$, $\chi^2(df = 5) = 123.000$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

Rules for using information systems

Table 4.65 depicts the view when the respondents were asked whether in a given organization there are rules (policy) for using IS (e-mail, the Internet, file-server, applications, LAN). The majority of respondents (82.1%: users of IS) revealed that organizations have implemented rules (policy) for using IS in an ad-hoc manner (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.65). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 124.231$, $p < .05$)

in Table 4.65 revealed that organizations should implement rules (policy) for using IS (e-mail, the Internet, file-server, applications, LAN). Thus, for enhancing the security of IS, organizations should implement rules (policy) for using IS.

Table 4.65: Rules/Policy For Using IS

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	6	15.4
1-Performed informally (unplanned)	32	82.1
3-Implementation is in progress (planned and tracked)	1	2.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 124.231, p = .000$, $\sum E_i = \sum O_i = N = 39$		

Access control policy for authorizing and revoking access rights

Table 4.66 presents findings on whether organizations have access control policy for authorizing and revoking access rights to IS (qn39). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.66). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have implemented access control policy for authorizing and revoking access rights to IS in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5. For, enhancing the security of IS, a given organization should implement an access control policy for authorizing and revoking access rights to IS.

Table 4.66: Access Control Policy for Authorizing And Revoking Access Rights

Security control	L	K	O	M	P	N	Q	Median/ Total
Access control policy for authorizing and revoking access rights (qn39)	1	0	1	1	0	0	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Process in place for granting and revoking appropriate user access

Table 4.67 presents findings on whether organizations have a process in place for granting and revoking appropriate user access (qn40). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.67). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have an ad-hoc (unplanned) process for granting and revoking appropriate user access; with a median of 1 in SSE-CMM rating scale of 0-5. For enhancing, the security of IS, a given organization should implement a process for granting and revoking appropriate user access.

Table 4.67: Process in Place for Granting and Revoking Appropriate User Access

Security control	L	K	O	M	P	N	Q	Median/ Total
Process in place for granting and revoking appropriate user access (qn40)	1	0	1	1	0	0	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Password management program that follows current security standards

Table 4.68 presents findings on whether a given organization had a password management program that follows current security standards (qn41). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.68). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed most organizations do not have a password management program that follows

current security standards; with a median of 0 in the SSE-CMM rating scale of 0-5.

Table 4.68: Password Management Program

Security control	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Password management program that follows current security standards(qn41)	1	0	0	1	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Procedures for reviewing access regularly

Table 4.69 presents findings on whether organizations have procedures for regularly reviewing users' access to ensure only needed privileges are applied (qn42). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.69). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations do not have procedures for reviewing users' access; with a median of 0 in the SSE-CMM rating scale of 0-5. For enhancing the security of IS, organizations should have procedures for regularly reviewing users' access to ensure only needed privileges are applied.

Table 4.69: Procedures to Regularly Review Access

Security control	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Procedures to regularly review access (qn42)	1	0	1	0	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Securing remote access

Table 4.70 presents findings on whether organizations have implemented controls to secure remote access services: use ssh, sftp, https (qn43). Semi-structured interviews were conducted in seven organizations involving 18 subject matter

experts (Head of ICT, IT staff) (Table 4.70). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have implemented controls for securing remote access services in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5. For enhancing the security of IS organizations, should implement specific controls to secure remote access services.

Table 4.70: Securing of Remote Access

Security control	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Securing of remote access (qn43)	1	0	1	1	0	0	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Prevent and detect rogue access to wireless-LANs

Table 4.71 presents findings on whether organizations have implemented specific controls to prevent and detect rogue access for all of the wireless LANs (qn44). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.71). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have not implemented specific controls for preventing and detecting rogue access to wireless LANs; with a median of 0 in the SSE-CMM rating scale of 0-5. For enhancing the security of IS, organizations should implement controls to prevent and detect rogue access for all of the wireless LANs.

Table 4.71: Prevent and Detect Rogue Access to Wireless-LANs

Security controls	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Prevent and detect rogue access to wireless-LANs (qn44)	1	0	0	0	0	1	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Block or restrict unencrypted sensitive information to untrusted networks

Table 4.72 presents findings on whether organizations employ technologies to block or restrict unencrypted sensitive information from travelling to untrusted networks (qn45). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.72). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have not employed technologies to block or restrict unencrypted sensitive information from travelling to untrusted networks; with a median of 0 in the SSE-CMM rating scale of 0-5. For enhancing the security of IS, organizations should employ technologies to block or restrict unencrypted sensitive information from travelling to untrusted networks.

Table 4.72: Restrict Unencrypted Sensitive Information to Untrusted Networks

Security control	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Block or restrict unencrypted sensitive information to untrusted networks(qn45)	0	0	0	0	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Restrict the sharing of passwords

Table 4.73 presents findings on whether organizations have a policy in place to restrict the sharing of passwords (qn46). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.73). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations do not have a policy for restricting the sharing of passwords; with a median of 0 in the SSE-CMM rating scale of 0-5. For enhancing the security of IS organizations, should have a policy in place to restrict the sharing of passwords.

Table 4.73: Restrict the Sharing of Passwords

Security control	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Restrict sharing of passwords (qn46)	1	0	1	1	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Authorization system to enforces time limits lockout on login failure

Table 4.74 presents findings on whether organizations have implemented an authorization system that enforces time limits lockout on login failure and defaults to minimum privileges (qn47). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.74). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have implemented authorization system for enforcing time limits lockout on login failure and which defaults to minimum privilege in ad-hoc (unplanned) manner; with a median of 1 in

SSE-CMM rating scale of 0-5.

Table 4.74: Authorization System That Enforces Time Limits Lockout On Login Failure

Security control	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Authorization system that enforces time limits lockout on login failure and defaults to minimum privileges (qn47).	1	1	0	1	0	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Policies and controls for the use of mobile devices

Table 4.75 presents findings on whether organizations have implemented policies and controls for the use of mobile devices: laptops, tablet PCs, smartphones, USB gadgets, removable storages and wearable ICT devices (qn48). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.75). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have not implemented policies and controls for the use of mobile devices; with a median of 0 in the SSE-CMM rating scale of 0-5. For enhancing the security of IS, organizations should have policies and controls for the use of mobile devices.

Table 4.75: Policies and controls for the use of mobile devices

Security controls	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Policies and controls for usage of mobile devices (qn48)	0	0	0	1	0	0	0	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Encryption of mobile computing devices

Table 4.76 presents findings on whether organizations require encryption on mobile computing devices: laptops, tablets (qn49). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.76). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations do not employ encryption on mobile computing devices; with a median of 0 in the SSE-CMM rating scale of 0-5. For enhancing the security of IS, organizations employ encryption on mobile computing devices.

Table 4.76: Encryption of Mobile Computing Devices

Security control	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Encryption on mobile computing devices (qn49)	0	0	0	0	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Telework policy that addresses multifactor access and endpoint security

Table 4.77 presents findings on whether organizations have implemented a telework policy that addresses multifactor access and security requirements for the endpoint used (qn50). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.77). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations do not have telework policy for addressing multifactor access and security requirements for the endpoint used; with a median of

0 in the SSE-CMM rating scale of 0-5. For enhancing the security of IS, organizations should implement a telework policy that addresses multifactor access and security requirements for the endpoint used.

Table 4.77: Telework policy

Security control	L	K	O	M	P	N	Q	Median/ Total
Telework policy that addresses multifactor access and end point security (qn50)	0	0	0	0	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

4.3.6 Cryptography

The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the existing cryptographic controls implementation in the education sector in Tanzania. The cryptographic controls involve cryptography policy and keys management control for enciphering and deciphering of secret data. It was hypothesized that effective implementation of cryptographic controls contributes to enhancing the security of IS.

Table 4.78 depicts the view when the respondents were asked whether organizations have implemented cryptography controls such as cryptographic policy and keys management. The majority of respondents (97.4%: IT staff) revealed that organizations have not implemented cryptographic controls (scale 0: non-existent); with a median of 0 in SSE-CMM (Table 4.78). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 183.308$, $p = .000$, $p < .05$) in Table 4.78 revealed that organizations should implement cryptographic controls. Thus, for enhancing the security of IS organizations, should implement cryptography controls (such as cryptographic policy and key management controls).

Table 4.78: Cryptography Controls

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	38	97.4
1-Performed informally (unplanned)	1	2.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 183.308, p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.3.7 Physical and Environmental Security

This assesses steps taken by organizations to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Both quantitative and qualitative data were collected. The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B). The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the physical and environmental controls. It was hypothesized that effective implementation of physical and environmental controls contributes to enhancing the security of IS.

Results findings for physical and environmental security controls assessments are summarized in Table 4.79. Furthermore, the detailed findings for security controls for physical and environmental security have been presented in the following paragraphs.

Table 4.79: Summary Results for Physical And Environmental Security

S/N	Security controls	Results
i	Physical and environmental security policy	Majority of respondents (69.2%: IT staff) revealed that organizations have implemented a physical and environmental security policy in an ad-hoc manner; with a median of 1 in SSE-CMM. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 95.308$, $p = .000$, $p < .05$) revealed that organizations should have an effective physical and environmental security policy.
ii	Restrict physical access to a sensitive area such as server rooms, data centres	Findings revealed that most organizations have implemented controls for restricting physical access to server rooms, data-centres to only authorized parties in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5.
iii	Protection of critical hardware and wiring from man-made and natural threats	Findings revealed that most organizations have implemented controls for protecting critical hardware and wiring from natural and man-made threats in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5.
iv	Background checks for access to sensitive facilities	The findings revealed that most organizations have implemented processes for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these sensitive facilities in an ad-hoc manner; with a median of 1 in SSE-CMM.
v	Media-sanitization process	Findings revealed that most organizations do not have a media-sanitization process that is applied to equipment prior to disposal, reuse, or release; with a median of 0 in the SSE-CMM rating scale of 0-5.

Physical and environmental security policy

Table 4.80 depicts the view when the respondents were asked whether organizations have a physical and environmental security policy in place. The majority of respondents (69.2%: IT staff) revealed that organizations have implemented a physical and environmental security policy in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.80). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 95.308$, $p = .000$, $p < .05$) in Table 4.80 revealed that organizations should have an effective physical and environmental security policy. Thus, for enhancing the security of IS organizations should implement a physical and environmental security policy.

Table 4.80: Physical and Environmental Security Policy

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	12	30.8
1-Performed informally (unplanned)	27	69.2
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2 (df = 5) = 95.308, p= .000$, $\sum E_i = \sum O_i = N = 39$		

Restrict physical access to a sensitive area

Table 4.81 presents findings on whether organizations server rooms, data centres include controls that ensure only authorized parties are allowed physical access (qn16). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.81). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have implemented controls for restricting physical access to server rooms, data centres to only authorized parties in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.81).

Table 4.81: Restrict Physical Access to A Sensitive Area

Security control	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Restrict physical access to sensitive area (qn16)	1	1	1	1	1	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Protection of critical hardware and wiring

Table 4.82 presents findings on whether organizations have implemented controls to protect critical hardware and wiring from natural and man-made threats (qn17). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.82). The semi-structured

interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have implemented controls for protecting critical hardware and wiring from natural and man-made threats in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.82).

Table 4.82: Protection of Critical Hardware and Wiring

Security Domain	L	K	O	M	P	N	Q	Median/ Total
Protection of critical hardware and wiring from man-made and natural threats (qn17)	1	1	1	1	1	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Background checks for access to sensitive facilities

Table 4.83 presents findings on whether a given organization has a process for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to sensitive facilities (qn18). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.83). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations have implemented processes for issuing keys, codes, and/or cards that require appropriate authorization and background checks for access to these sensitive facilities in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.83).

Table 4.83: Background Checks for Access to Sensitive Facilities

Security control	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Background checks for access to sensitive facilities when issuing keys, codes, cards (qn18)	1	0	1	1	0	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Media-sanitization process

Table 4.84 presents findings on whether a given institution had a media-sanitization process that is applied to equipment prior to disposal, reuse, or release (qn19). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.84). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations do not have a media-sanitization process that is applied to equipment prior to disposal, reuse, or release; with a median of 0 in the SSE-CMM rating scale of 0-5. For enhancing the security of IS, organizations should perform media-sanitization to equipment prior to disposal, reuse, or release.

Table 4.84: Media-Sanitization Process

Security control	Organisation							Median/ Total
	L	K	O	M	P	N	Q	
Media-sanitization process (qn19)	1	0	0	0	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

4.3.8 Communications Security

This assesses communication security controls in IS, the case of the education sector in Tanzania. It includes network security management controls (network controls, the security of network services, and segregation in networks); information transfer controls (information transfer policies and procedures, agreements on information transfer, electronic messaging, confidentiality or non-disclosure agreements). The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B). The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of

fit test with 0.05 significance level and $df = 5$ was carried out to assess the communication security controls implementation in the education sector in Tanzania.

It was hypothesized that effective implementation of communication security controls contributes to enhancing the security of IS. Results findings for operation security controls assessments are summarized in Table 4.98. Furthermore, the detailed findings for security controls for operation security have been presented in the following paragraphs.

Table 4.98: Summary Results for Communication Security Controls

S/N	Security controls	Results
i	Network security policy	The majority of respondents (66.7%: IT staff) revealed that most organizations have implemented network security policy in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale 0-5. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 87.308, p = .000, p < .05$) revealed that to enhance the security of IS, organizations should implement a network security policy.
ii	Segmented network architecture	The findings revealed that most organizations do not have segmented network architecture; with a median of 0 in the SSE-CMM rating scale of 0-5.
iii	Internet-accessible servers are protected by more than one security layer	The findings revealed that most organizations protect their Internet-accessible servers by more than one security layer in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5.
iv	Use of appropriate vetted encryption methods to protect sensitive data in transit	The findings revealed that most organizations do not use appropriate vetted encryption methods to protect their sensitive data in transit; with a median of 0 in the SSE-CMM rating scale of 0-5.
v	Policies and procedures to protect the exchange of information	The findings revealed that most organizations do not have policies and procedures in place to protect the exchange of information within their organizations and with third-party agreements; with a median of 0 in SSE-CMM rating scale of 0-5.
vi	Protecting data related to e-commerce while traversing public networks	The findings revealed that most organizations do not have a process protecting data related to e-commerce traversing public networks; with a median of 0 in the SSE-CMM rating scale of 0-5.

Network security policy

Table 4.99 depicts the view when the respondents were asked whether organizations have organizations have implemented a network security policy. The majority of respondents (66.7%: IT staff) revealed that organizations have implemented network

security policy in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.99). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 87.308$, $p = .000$, $p < .05$) in Table 4.99 revealed that organizations should implement network security policy. Thus, for enhancing the security of IS organizations should implement a network security policy.

Table 4.99: Network Security Policy

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	12	30.8
1-Performed informally (unplanned)	26	66.7
2-Partially implemented (planned)	1	2.6
Total	39	100.0
Median=1, E_i per category $i = 1/6 * 39 = 6.5$, $\chi^2(df = 5) = 87.308$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

Segmented network architecture

Table 4.100 presents findings on whether organizations have segmented network architecture to provide different levels of security based on the information's classification (qn31). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.100 revealed that most organizations do not have a segmented network architecture; with a median of 0 in the SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should implement segmented network architecture for providing different levels of security based on the information's classification.

Table 4.100: Segmented Network Architecture

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Segmented network architecture to provide different levels of security based on the information's classification (qn31).	1	0	0	2	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Internet-accessible servers are protected by more than one security layer

Table 4.101 presents findings on whether organizations Internet-accessible servers are protected by more than one security layer: firewalls, network IDS, host IDS, application IDS, DMZ (qn32). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.101 revealed that most organizations protect their Internet-accessible servers by more than one security layer in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS, organizations should protect their Internet-accessible servers by more than one security layer.

Table 4.101: Internet-Accessible Servers Are Protected

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Internet-accessible servers are protected by more than one security layer: firewalls, network IDS, host IDS, application IDS, DMZ (qn32)	1	1	0	1	0	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Use of appropriate vetted encryption methods to protect sensitive data in transit

Table 4.102 presents findings on whether organizations use appropriate/vetted encryption methods to protect their sensitive data in transit (qn33). The semi-

structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.102 revealed that most organizations do not use appropriate/vetted encryption methods to protect their sensitive data in transit; with a median of 0 in the SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should use appropriate/vetted encryption methods to protect their sensitive data in transit.

Table 4.102: Appropriate Encryption Methods to Protect Sensitive Data in Transit

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Use of appropriate vetted encryption methods to protect their sensitive data in transit (qn33).	0	0	0	1	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Policies and procedures to protect the exchange of information

Table 4.103 presents findings on whether organizations have policies and procedures in place to protect the exchange of information (within the organization and with third-party agreements) from interception, copying, modification, misrouting, and destruction (qn34). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.103 revealed that most organizations do not have policies and procedures in place to protect the exchange of information within their organizations and with third-party agreements; with a median of 0 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should have policies and procedures in place to protect the exchange of information (within their organizations and with third-party agreements) from interception, copying, modification, misrouting, and destruction.

Table 4.103: Policies and procedures to protect the exchange of information

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Policies and procedures in place to protect the exchange of information (within the organization and with third-party agreements) from interception, copying, modification, misrouting, and destruction (qn34).	0	0	0	1	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Protecting data related to e-commerce while traversing public networks

Table 4.104 presents findings on whether an organization has a process in place to ensure data related to electronic commerce (e-commerce) traversing public networks are protected from fraudulent activity, unauthorized disclosure or modification (qn35). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed.

The findings in Table 4.104 revealed that most organizations do not have a process in place for protecting data related to e-commerce while traversing public networks from fraudulent activity, unauthorized disclosure, or modification; with a median of 0 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should have a process in place to ensure data related to e-commerce traversing public networks are protected from fraudulent activity, unauthorized disclosure or modification.

Table 4.104: Protecting E-Commerce Data Traversing Public Networks

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Process in place to ensure data related to electronic commerce (e-commerce) traversing public networks are protected from fraudulent activity, unauthorized disclosure or modification (qn35)	0	0	0	0	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

4.3.9 System Acquisition, Development and Maintenance

This assesses the effectiveness of system acquisition, development and maintenance controls in IS, the case of the education sector in Tanzania. It includes security requirements of IS; security controls in development and support processes; and security controls for test data. The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B). The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried to assess the system acquisition, development and maintenance security controls implementation in the education sector in Tanzania.

It was hypothesized that effective implementation of system acquisition, development, and maintenance of security controls contribute to enhancing the security of IS. Its results findings are summarized in Table 4.105. Furthermore, the detailed findings for security controls for system acquisition, development and maintenance have been presented in the following paragraphs.

Table 4.105: Summary Results for System Acquisition, Development and Maintenance

S/N	Security controls	Results
i	Acquisition, development and maintenance policy	The majority of respondents (76.9%: IT staff) revealed that most organizations have implemented acquisition, development and maintenance policy in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 111.923, p = .000, p < .05$) revealed that organizations should implement the acquisition, development and maintenance policy.
ii	New IS or enhanced IS security requirements validation	The findings revealed that most organizations do not validate new IS or enhancements to existing IS against defined security requirements; with a median of 0 in the SSE-CMM rating scale of 0-5

S/N	Security controls	Results
iii	Standards that address secure coding practices	The findings revealed that most organizations do not employ standards that address secure coding practices with a median of 0 in the SSE-CMM rating scale of 0-5
iv	Validation checks to ensure data output is as expected	The findings revealed that most organizations do not have validation checks for ensuring that data outputs from IS are as expected; with a median of 0 in the SSE-CMM rating scale of 0-5.
v	Policies to indicate when encryption should be used	The findings revealed that in most organizations policies do not indicate when encryption should be used; with a median of 0 in the SSE-CMM rating scale of 0-5.
vi	The configuration management process for changes to its critical systems	The findings revealed that most organizations do not have configuration management process for ensuring that changes to their critical systems are for the valid business reasons and have received proper authorization; with a median of 0 in SSE-CMM rating scale of 0-5
vii	Perform reviews and tests to changes made to production systems	The findings revealed that most organizations do not perform reviews and tests for the changes made to production systems; with a median of 0 in the SSE-CMM rating scale of 0-5.
viii	Security requirements for outsourced software development	The findings revealed that most organizations do not include security requirements in contract agreements for outsourced software development; with a median of 0 in the SSE-CMM rating scale of 0-5
iv	Patch management strategy for monitoring and responding to patch releases	The findings revealed that most organizations do not have a patch management strategy in place and responsibilities has yet not assigned; with a median of 0 in the SSE-CMM rating scale of 0-5.

Acquisition, development and maintenance policy

Table 4.106 depicts the view when the respondents were asked whether organizations have implemented the acquisition, development and maintenance policy. The majority of respondents (76.9%: IT staff) revealed that most organizations have implemented acquisition, development and maintenance policy in ad-hoc (scale 1: unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.106). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 111.923$, $p = .000$, $p < .05$) in Table 4.106 revealed that organizations should implement the acquisition, development and maintenance policy. Thus, for enhancing the security of IS; organizations should implement the acquisition, development and maintenance policy.

Table 4.106: Acquisition, development and maintenance policy

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	9	23.1
1-Performed informally (unplanned)	30	76.9
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 111.923$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

New IS or enhanced IS security requirements validation

Table 4.107 presents findings on whether new IS or enhancements to existing IS in a given organization are validated against defined security requirements (qn51). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations do not validate new IS or enhancements to existing IS against defined security requirements; with a median of 0 in the SSE-CMM rating scale of 0-5 (Table 4.107). For enhancing the security of IS, organizations should validate new IS or enhancements to existing IS against defined security requirements.

Table 4.107: New IS or enhanced IS security requirements validation

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
New IS or enhanced IS security requirements validation (qn51)	1	0	1	0	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Standards that address secure coding practices

Table 4.108 presents findings on whether organizations have established standards that address secure coding practices (e.g., input validation, proper error handling, session management, etc.), and take into consideration common application security

vulnerabilities (e.g., CSRF, XSS, code injection, etc.) (qn52). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.108 revealed that most organizations have not employed standards that address secure coding practices that take into consideration common application security vulnerabilities (e.g., CSRF, XSS, code injection, etc.); with a median of 0 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should establish standards that address secure coding practices and take into consideration common application security vulnerabilities in the established standards.

Table 4.108: Standards that address secure coding practices

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Standards that address secure coding practices (qn52).	0	0	0	1	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Validation checks to ensure data output is as expected

Table 4.109 presents findings on whether organizations have validation checks to ensure data output is as expected; as the incorrect output may occur even in tested systems (qn53). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.109 revealed that most organizations do not validation checks for ensuring that data outputs from IS are as expected; with a median of 0 in the SSE-CMM rating scale of 0-5. Thus, for enhancing the security of

ISs organizations should have validation checks for ensuring that outputs from acquired/developed IS are as expected.

Table 4.109: Validation Checks to Ensure Data Output is as Expected

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Validation checks to ensure data output is as expected; as incorrect output may occur even in tested systems (qn53)	1	0	1	1	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Policies to indicate when encryption should be used

Table 4.110 presents findings on whether policies in a given organization indicate when encryption should be used (e.g., at rest, in transit, with sensitive or confidential data, etc.) (qn54). The semi-structured interview employed data collection matrix tool (Appendix B). The findings in Table 4.110 revealed that most organizations policies do not indicate when encryption should be used; with a median of 0 in the SSE-CMM rating scale of 0-5. Thus, for enhancing the security of ISs policies in organizations should indicate when encryption should be used (e.g., at rest, in transit, with sensitive or confidential data, etc.).

Table 4.110: Policies to Indicate When Encryption Should be Used

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Policies to indicate when encryption should be used (qn54)	0	0	0	0	0	1	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

The configuration management process for changes to its critical systems

Table 4.111 presents findings on whether organizations have configuration management process in place to ensure that changes to its critical systems are for valid business reasons and have received proper authorization (qn55). The semi-structured interview employed data collection matrix tool (Appendix B). The

findings in Table 4.111 revealed that most organizations do not have a configuration management process in place for ensuring that changes to their critical systems are for the valid business reasons and have received proper authorization; with a median of 0 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should have a configuration-management process in place for ensuring that changes to their critical systems are for the valid business reasons and have received a proper authorization.

Table 4.111: Configuration Management Process for Changes to its Critical Systems

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Configuration management process to ensure that changes to its critical systems are for valid business reasons and have received proper authorization (qn55).	0	0	1	1	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Perform reviews and tests to changes made to production systems

Table 4.112 presents findings on whether organizations perform reviews and tests to changes made to production systems in order to ensure that they do not have an adverse impact on security or operations (qn56). The semi-structured interview employed data collection matrix tool (Appendix B). The findings in Table 4.112 revealed that most organizations do not perform reviews and tests for the changes made to production systems; with a median of 0 in the SSE-CMM rating scale of 0-5. Thus, enhancing the security of IS organizations should perform reviews and tests for the changes made to production systems in order to ensure that they do not have an adverse impact on security or operations.

Table 4.112: Perform Reviews and Tests to Changes Made to Production Systems

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Performs reviews and tests to changes made to production systems in order to ensure that they do not have an adverse impact on security or operations (qn56). Qn56	0	0	1	1	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Security requirements for outsourced software development

Table 4.113 presents findings on whether organizations include security requirements in contract agreements for outsourced software development (qn57). The semi-structured interview employed data collection matrix tool (Appendix B). The findings in Table 4.113 revealed that most organizations do not include security requirements in contract agreements for outsourced software development; with a median of 0 in the SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should include security requirements in contract agreements for outsourced software development.

Table 4.113: Security Requirements for Outsourced Software Development

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Security requirements in contract agreements for outsourced software development (qn57)	0	0	0	1	0	1	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Patch management strategy for monitoring and responding

Table 4.114 presents findings on whether the organisation has a patch management strategy in place and responsibilities has been assigned for monitoring and promptly responding to patch releases, security bulletins, and vulnerability reports (qn58). The semi-structured interview employed data collection matrix tool (Appendix B). The

findings in Table 4.114 revealed that most organizations do not have a patch management strategy in place and responsibilities has been not been assigned; with a median of 0 in the SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should have a patch management strategy in place and responsibilities should be assigned for monitoring and promptly respond to patch releases, security bulletins, and vulnerability reports.

Table 4.114: Patch management for monitoring and responding to patch releases

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Patch management strategy for monitoring and promptly responding to patch releases, security bulletins, and vulnerability (qn58)	1	0	0	1	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

4.3.10 Supplier Relationships

This assesses the effectiveness of supplier relationships controls in IS, the case of the education sector in Tanzania. It includes security in supplier relationship (information security policy for supplier relationships, security within supplier agreements and ICT supply chain) and supplier service delivery management (monitoring and review of supplier services, and managing changes to supplier services). The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the effectiveness of supplier relationships controls implementation case of the education sector in Tanzania. It was hypothesized that effective implementation of supplier relationships controls contributes to enhancing the security of IS. The results findings are as follows.

Table 4.115 depicts the view when the respondents were asked whether organizations have implemented policies, and procedures for managing suppliers relationships. The majority of respondents (61.5%: IT staff) revealed that organizations have implemented policies and procedures for managing suppliers relationships in ad-hoc (scale 1: unplanned); with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.115).

Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 87.308$, $p = .000$, $p < .05$) in Table 4.115 revealed that organizations should implement policies, procedures for managing suppliers relationships. Thus, for enhancing the security of is organizations should implement policies and procedures for managing suppliers relationships.

Table 4.115: Policies, Procedures for Managing Suppliers' Relationships

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	14	35.9
1-Performed informally (unplanned)	24	61.5
2-Partially implemented (planned)	1	2.6
Total	39	100.0
Median=1, E_i per category $i = 1/6 * 39 = 6.5$, $\chi^2(df = 5) = 87.308$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.3.11 Information Security Incident Management

This assesses the effectiveness of management of information security incidents controls for improving security in IS, the case of the education sector in Tanzania. It includes responsibilities and procedures; reporting information security events and weaknesses; assessment and decision of information security events. Moreover, it involves a response to information security incidents, learning from information

security incidents and the collection of evidence for the potential investigation. The quantitative data were collected through survey questionnaires (Appendix B).

The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B). The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the information security incident management control implementation in the education sector in Tanzania. It was hypothesized that effective implementation of information security incident management controls contributes to enhancing the security of IS. The results are as follows.

Table 4.116 presents findings on whether organizations have implemented incident-handling procedures for reporting and responding to security events throughout the incident lifecycle, including the definition of roles and responsibilities (qn59). The semi-structured interview employed data collection matrix tool (Appendix B). The findings revealed that most organizations do not incident-handling procedures; with a median of 0 in the SSE-CMM rating scale of 0-5 (Table 4.116). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 84.231, p = .000, p < .05$) revealed that organizations should implement incident-handling procedures for reporting and respond to security events throughout the incident lifecycle (Section 4.2.3.2). For enhancing the security of IS organizations should have incident-handling procedures for reporting and respond to security events throughout the incident lifecycle, including the definition of roles and responsibilities.

Table 4.116: Incident Handling Policies and Procedures Throughout its Life Cycle

Security Control	Organization							Median/ Total
	L	K	O	M	P	N	Q	
Incident handling policies and procedures for reporting and responding to security events throughout the incident lifecycle, including the definition of roles and responsibilities (qn59)	0	0	0	1	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

4.3.12 Operations Security

This assesses the effectiveness of operational security controls in IS, the case of the education sector in Tanzania. It includes operational procedures and responsibilities, protection from malware, back-up, logging, and monitoring to record events and generates evidence, control of operational software, and information systems audit consideration. The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B). The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the operational security controls implementation.

Table 4.117: Summary Results for Operation Security

S/N	Security controls	Results
i	Change management policy and acceptable use policy	Majority of respondents (51.3%: IT staff) revealed that organizations have implemented change management policy and acceptable use policy in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5. Moreover, Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 55.308, p < .05$) revealed that to enhance the security of IS, organizations should implement change management policy and acceptable use policy for information resources.
ii	Security configuration standards for IS and applications	The findings revealed that most organizations maintain security configuration standards for IS and applications in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5.
iii	Changes to IS are tested, authorized and reported	The findings revealed that most changes to IS are tested, authorized and reported in ad-hoc (unplanned) manner; with a

S/N	Security controls	Results
		median of 1 in SSE-CMM rating scale of 0-5.
iv	Duties are sufficiently segregated	The findings revealed that in most organizations duties are not segregated to ensure unintentional or unauthorized modification of information is detected; with a median of 0 in the SSE-CMM rating scale of 0-5.
v	Production systems are separated from other stages of the development life cycle	The findings revealed that in most organizations production systems are separated from other stages of the development lifecycle in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5.
vi	Monitor the utilization of key systems resources	The findings revealed that most organizations have implemented processes for monitoring the utilization of key systems resources and mitigation of downtime systems risk in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5.
vii	Methods for detecting and eradicating known malicious code	The findings revealed that most organizations have ad-hoc (unplanned) methods for detecting and eradicating known malicious code; with a median of 1 in SSE-CMM rating scale of 0-5.
viii	Backup procedures	The findings revealed that most organizations have ad-hoc (unplanned) backup procedures for taking backups; with a median of 1 in SSE-CMM rating scale of 0-5.
ix	A routine test of restore procedures	The findings revealed that most organizations test their restore procedures in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5.
x	Logging automatically security-related activities such as access attempts, hardware, and software changes	The findings revealed that most organizations do not automatically log security-related activities; with a median of 0 in the SSE-CMM rating scale of 0-5
xi	Routinely monitoring of logs	The findings revealed that most organizations do not have a process for routinely monitoring logs to detect unauthorized and anomalous activities; with a median of 0 in the SSE-CMM rating scale of 0-5.
xii	File-integrity monitoring tools for alerting personnel on unauthorized modification	The findings revealed that most organizations do not have file-integrity monitoring tools; with a median of 0 in the SSE-CMM rating scale of 0-5.

It was hypothesized that the implementation of operations security controls, enhance the security of IS. Results findings for operation security controls assessments are summarized in Table 4.117. Furthermore, the detailed findings for security controls for operation security have been presented in the following paragraphs.

Change management policy and acceptable use policy

Table 4.118 depicts the view when the respondents were asked whether organizations have implemented change management policy and acceptable use policy for information resources. The majority of respondents (51.3%: IT staff)

revealed that organizations have implemented change management policy and acceptable use policy in ad-hoc (scale 1: unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.118). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 55.308, p < .05$) in Table 4.118 revealed that organizations should implement change management policy and acceptable use policy for information resources. Thus, for enhancing the security of IS organizations should implement effective and efficient change management policy and acceptable use policy for information resources.

Table 4.118: Change Management Policy and Acceptable Use Policy

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	14	35.9
1-Performed informally (unplanned)	20	51.3
2-Partially implemented (planned)	4	10.3
3-Implementation is in progress (planned and tracked)	1	2.6
Total	39	100.0
Median=1, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 55.308, p = .000, \sum E_i = \sum O_i = N = 39$		

Security configuration standards for IS and applications

Table 4.119 presents findings on whether institutions maintain security configuration standards for IS and applications (qn20). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.119). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings revealed that most organizations maintain security configuration standards for IS and applications in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.119).

Table 4.119: Security Configuration Standards for IS and Applications

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Maintain security configuration standards for IS and applications (qn20)	1	0	1	1	0	0	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Changes to IS are tested, authorized and reported

Table 4.120 presents findings on whether changes to IS institutions are tested authorized and reported (qn21). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.120). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.120 revealed that most changes to IS are tested, authorized and reported in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5.

Table 4.120: Changes to IS are Tested, Authorized And Reported

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Changes to IS institutions are tested authorized and reported (qn21)	1	1	1	1	0	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Duties are sufficiently segregated

Table 4.121 presents findings on whether duties in a given organization are sufficiently segregated to ensure unintentional or unauthorized modification of information is detected (qn22). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.121). The semi-structured interview employed data collection matrix tool

(Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.121 revealed that in most organizations duties are not segregated to ensure unintentional or unauthorized modification of information is detected; with a median of 0 in the SSE-CMM rating scale of 0-5.

Table 4.121: Duties are Sufficiently Segregated

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Duties are sufficiently segregated (qn22)	0	0	0	1	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Production systems are separated from other stages of the development life cycle

Table 4.122 presents findings on whether a given organization production systems are separated from other stages of the development life cycle (qn23). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.122). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.122 revealed that in most organizations production systems are separated from other stages of the development lifecycle in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS production systems should be separated from other stages of the development lifecycle.

Table 4.122: Production Systems are Separated from Other Stages

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Production systems are separated from other stages of the development life cycle (qn23)	1	1	1	2	0	0	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Monitor the utilization of key systems resources

Table 4.123 presents findings on whether organizations have processes in place to monitor the utilization of key systems resources and to mitigate the risk of systems downtime (qn25). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.123). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.123 revealed that most organizations have implemented processes for monitoring the utilization of key systems resources and mitigation of downtime systems risk in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should have processes in place for monitoring the utilization of key systems resources and mitigation of risk of systems downtime.

Table 4.123: Monitor The Utilization of Key Systems Resources

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Monitor the utilization of key systems resources and to mitigate the risk of systems downtime (qn25)	1	1	1	1	0	0	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Methods for detecting and eradicating known malicious code

Table 4.124 presents findings on whether organizations have methods for detecting and eradicating known malicious code transported by electronic mail, the web, computers, mobile computing devices or removable media (qn26). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.124). The semi-structured interview

employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed.

The findings in Table 4.124 revealed that most organizations have ad-hoc (unplanned) methods for detecting and eradicating known malicious code transported by electronic mail, the web, computers, mobile computing devices or removable media; with a median of 1 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should have methods for detecting and eradicating known malicious code transported by electronic mail, the web, computers, mobile computing devices or removable media.

Table 4.125: Methods for Detecting and Eradicating Known Malicious Code

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Methods for detecting and eradicating known malicious code transported by electronic mail, the web, computers, mobile computing devices or removable media (qn26)	1	1	1	2	1	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Backup procedures

Table 4.126 presents findings on whether an organization has backup procedures for taking backups consistently (qn27). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.126). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.126 revealed that most organizations have ad-hoc (unplanned) backup procedures for taking backups; with a median of 1 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should have backup procedures for taking backups consistently.

Table 4.126: Backup Procedures

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Backup procedures for taking backups consistently (qn27)	1	1	1	2	1	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

A routine test of restore procedures

Table 4.127 presents findings on whether an organization performs a routine test of their restore procedures (qn28). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.127). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.127 revealed that most organizations test their restore procedures in ad-hoc (unplanned) manner; with a median of 1 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organization should perform a routine test of their restore procedures.

Table 4.127: Routine Test of Restore Procedures

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Performs a routine test of their restore procedures (qn28).	1	1	1	1	0	1	1	1
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Logging automatically security-related activities

Table 4.128 presents findings on whether organizations security-related activities such as hardware configuration changes, software configuration changes, access attempts, authorization/privilege assignments are automatically logged (qn36). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.128).

The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.128 revealed that most organizations do not automatically log security-related activities such as hardware configuration changes, software configuration changes, access attempts, authorization/privilege assignments; with a median of 0 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization/privilege assignments should be automatically logged.

Table 4.128: Logging Automatically Security-Related Activities

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Security-related activities such as hardware and software configuration changes, access attempts are automatically logged (qn36).	1	0	0	1	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Routinely monitoring of logs

Table 4.129 presents findings on whether an organization has a process for routinely monitoring logs to detect unauthorized and anomalous activities (qn37). Semi-structured interviews were conducted in seven organizations involving 18 subject matter experts (Head of ICT, IT staff) (Table 4.129). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed. The findings in Table 4.129 revealed that most organizations do not have a process for routinely monitoring of logs to detect unauthorized and anomalous activities; with a median of 0 in the SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS

organizations should have a process for routinely monitoring logs to detect unauthorized and anomalous activities.

Table 4.129: Routinely Monitoring of Logs

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
Process for routinely monitoring logs to detect unauthorized and anomalous activities (qn37)	1	0	0	1	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

File-integrity monitoring tools for alerting on unauthorized

Table 4.130 presents findings on whether organizations have file-integrity monitoring tools for alerting personnel on unauthorized modification of critical system files, configuration files or content files, and the organization has software which is configured to perform critical file comparisons at least weekly (qn38). The semi-structured interview employed data collection matrix tool (Appendix B). The data collected through a semi-structured interview were cleaned, coded and analyzed.

The findings in Table 4.130 revealed that most organizations do not have file-integrity monitoring tools and software are not configured to perform critical file comparisons at least weekly; with a median of 0 in SSE-CMM rating scale of 0-5. Thus, for enhancing the security of IS organizations should have file-integrity monitoring tools for alerting personnel on unauthorized modification of critical system files, configuration files or content files, and software configured to perform critical file comparisons at least weekly.

Table 4.130: File-Integrity Monitoring Tools for Alerting

Security domain	Organisation							Total/ Median
	L	K	O	M	P	N	Q	
File-integrity monitoring tools for alerting personnel on unauthorized modification of critical system files, configuration files or content files, and the organization has software which is configured to perform critical file comparisons at least weekly (qn38)	0	0	0	0	0	0	1	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

4.3.13 Business Continuity

This assesses the effectiveness of existing business continuity controls, case of the education sector in Tanzania. It includes information security aspects of business continuity management and redundancies. The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B). The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the business continuity controls implementation, the case of the education sector in Tanzania. It was hypothesized that effective implementation of business continuity controls contributes to enhancing the security of IS. The result is as follows.

Table 4.131 presents findings on whether an organization has a documented business continuity plan that is based on a business impact analysis, is periodically tested, and it has been reviewed and approved by top management or the board of trustees (qn61). The semi-structured interview employed data collection matrix tool (Appendix B). The findings revealed that most organizations do not have documented business continuity plan with a median of 0 in SSE-CMM rating scale

of 0-5 in Tanzania education sector. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 67.615$, $p < .05$) revealed that should implement effective controls for information security aspects of business continuity management and redundancies (Section 4.2.3.1). For enhancing the security of IS organizations should implement effective controls for information security aspects of business continuity management and redundancies for the availability of IS and information processing facilities.

Table 4.131: Business Continuity Plan Controls

Security Domain	Organization							Median/ Total
	L	K	O	M	P	N	Q	
A given organization has a documented business continuity plan that is based on a business impact analysis, is periodically tested, and it has been reviewed and approved by top management or the board of trustees (qn61).	1	0	0	0	1	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

4.3.14 Compliance

This assesses the effectiveness of compliance controls, case of the education sector in Tanzania. It includes standard operating procedures evaluation for compliance and IS vulnerability testing or penetration testing. The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B). The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the effectiveness of compliance controls implementation, the case of the education sector in Tanzania. It was hypothesized that effective implementation of security controls for compliance contributes to

enhancing the security of IS. Its results findings are summarized in Table 4.132. Furthermore, the detailed findings for security controls for compliance have been presented in the following paragraphs.

Table 4.132: Summary Results for Compliance Controls

S/N	Security controls	Results
i	Standard operating procedures evaluation for compliance	The majority of respondents (87.2%) revealed that organizations are not evaluated for compliance with information security policies, standards, and procedures; with a median of 0 in the SSE-CMM rating scale of 0-5. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39)=142.692$, $p<.05$) revealed that organizations should be evaluated for compliance with information security policies, standards, and procedures.
ii	IS vulnerability testing or penetration testing	The majority of respondents (76.9%: IT staff) revealed that organizations do not perform application/network layer vulnerability testing or penetration testing against critical IS (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale of 0-5. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39)=111.923$, $p<.05$) revealed that organizations should perform application or network layer vulnerability testing or penetration testing against critical IS.

Standard operating procedures evaluation for compliance

Table 4.133 presents findings on whether the organizations are evaluated for compliance with information security policies, standards, and procedures. The majority of respondents (87.2%: IT staff) revealed that organizations are not evaluated for compliance with information security policies, standards, and procedures (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.133). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39)=142.692$, $p<.05$) in Table 4.133 revealed that organizations should be evaluated for compliance with information security policies, standards, and procedures. Thus, enhancing the security of IS organizations should be evaluated for compliance with information security policies, standards, and procedures.

Table 4.133: Evaluation of Compliance With Security Policies and Standards

SSE-CMM level	Observation N	Percent
0-Not performed (non-existent)	34	87.2
1-Performed informally (unplanned)	5	12.8
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 142.692$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

Information Systems vulnerability testing or penetration testing

Table 4.134 presents findings on whether organizations perform periodic application and network layer vulnerability testing or penetration testing against critical IS. The majority of respondents (76.9%: IT staff) revealed that organizations do not perform application/network layer vulnerability testing or penetration testing against critical IS (scale 0: non-existent); with a median of 0 in SSE-CMM rating scale of 0-5 (Table 4.120). Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 39) = 111.923$, $p < .05$) in Table 4.134 revealed that organizations should perform application or network layer vulnerability testing or penetration testing against critical IS. Thus, for enhancing the security of IS, organizations should perform application or network layer vulnerability testing or penetration testing against critical IS.

Table 4.134: Application and network layer vulnerability or penetration testing

SSE-CMM level	Observed N	Percent
0-Not performed (non-existent)	30	76.9
1-Performed informally (unplanned)	9	23.1
Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5) = 111.923$, $p = .000$, $\sum E_i = \sum O_i = N = 39$		

4.3.15 Risk Management

This section presents an assessment of the effectiveness of existing controls for risk management, a case study of the education sector in Tanzania. The study was carried

out to assess the risk management process as it relates to creating an information security strategy and program for enhancing IS security. Information security risk management is a major subset of the risk management process, which includes not only assessing information security risks to the institution but also determining appropriate management action and setting priorities for managing and implementing controls to protect against those risks. The quantitative data were collected through survey questionnaires (Appendix B). The qualitative data were collected through a semi-structured interview using interview data collection matrix (Appendix B). The quantitative data were analyzed and statistically tested using Chi-square goodness of fit test. The Chi-square goodness of fit test with 0.05 significance level and $df = 5$ was carried out to assess the security controls implementations for risk management, the case of the education sector in Tanzania.

It was hypothesized that effective implementation of risk management controls contributes to enhancing the security of IS. Its results findings are summarized in Table 4.135. Furthermore, the detailed findings for risk management controls have been presented in the following paragraphs.

Table 4.135: Summary Results for Risk Management Controls

S/N	Security controls	Results
i	The risk management program and risk register	Findings revealed that most organizations do not have a risk management program and risk register; with a median of 0 in the SSE-CMM rating scale of 0-5.
ii	Reviewing and updating risk register regularly	The majority of respondents (88%: management staff; 92% IT staff) revealed that most organizations do not review and update risk register or they do in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 50) = 71.440, p < .05$) revealed that organizations should review and update the risk register regularly.
iii	Conducts routine risk assessments	Findings reveal that most organizations do not conduct routine risk assessments; with a median of 0 in the SSE-CMM rating scale of 0-5.

The risk management program and risk register

Table 4.136 presents findings on whether a given organization has a risk management program and risk register (qn1). The semi-structured interview employed data collection matrix tool (Appendix B). The findings in Table 4.136 reveal that most organizations do not have a risk management program and risk register; with a median of 0 in SSE-CMM rating scale of 0-5 in Tanzania education sector. Thus, for enhancing the security of IS organizations should have a risk management program and risk registers.

Table 4.136: Risk Management Program and Risk Register

Security Domain	Organization							Median/ Total
	K	L	M	N	O	P	Q	
Risk management program and risk register(qn1)	0	0	5	5	0	0	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

Reviewing and updating risk register regularly

Table 4.137 depicts the view when the respondents were asked whether the organization has a risk register which is regularly reviewed and updated. The majority of respondents (88%: management staff) revealed that most organizations do not review and update risk register or they do in an ad-hoc manner; with a median of 1 in SSE-CMM rating scale of 0-5 (Table 4.137). The same question was asked to IT staff, the majority of respondents (92.3%: IT staff) revealed that organisations do not review and update risk register (scale 0: non-existent); or they do in ad-hoc manner; with a median of 1 in SSE-CMM rating scale 0-5 (Table 4.137). Moreover, the Chi-square goodness of fit test results (management staff: $\chi^2(5, N = 50) = 71.440$, $p < .05$; IT staff: $\chi^2(5, N = 39) = 61.769$, $p < .05$) in Table 4.137 revealed that organizations should review and update risk register regularly. Thus, for enhancing the security of IS organizations should review and update risk register regularly.

Table 4.137: Risk Register Reviewed and Updated

	SSE-CMM level	Observed N	Percent
Management staff: Risk register			
	0-Not performed (non-existent)	19	38.0
	1-Performed informally (unplanned)	25	50.0
	2-Partially implemented (planned)	5	10.0
	3-Implementation is in progress (planned and tracked)	1	2.0
	Total	50	100.0
Median=0, E_i per category $i=1/6*50=8.3$, $\chi^2(df = 5)=71.440$, $p=.000$, $\sum E_i = \sum O_i = N = 50$			
IT staff: Risk register			
	0-Not performed (non-existent)	19	48.7
	1-Performed informally (unplanned)	17	43.6
	2-Partially implemented (planned)	2	5.1
	3-Implementation is in progress (planned and tracked)	1	2.6
	Total	39	100.0
Median=0, E_i per category $i=1/6*39=6.5$, $\chi^2(df = 5)=61.769$, $p=.000$, $\sum E_i = \sum O_i = N = 39$			

Conducts routine risk assessments

Table 4.138 presents findings on whether a given organization conducts routine risk assessments to identify the key objectives that need to be supported by the information security program (qn2). The qualitative data were collected using semi-structured interview employed data collection matrix tool (Appendix B). The findings reveal that most organizations do not conduct routine risk assessments; with a median of 0 in the SSE-CMM rating scale of 0-5.

Table 4.138: Conducts Routine Risk Assessments

Security Domain	Organization							Median/ Total
	K	L	M	N	O	P	Q	
Conducts routine risk assessments to identify the key objectives that need to be supported by the information security program (qn2).	1	0	1	0	0	1	0	0
Respondents : Head of ICT & IT Staff	2	1	1	4	3	3	4	18

4.4 Improving the Security of Information and Information Systems

The study carried out an assessment of the institutions' information security maturity level and determined the applicable security controls to be implemented for improving IS security. The data were collected through document review and a semi-structured interview with a focused group (subject matter experts). The interview discussion for each organization (K, L, M, N, O, P, and Q) was captured using the electronic assessment tool, and open-ended questions responses were captured in the separate template in the laptop. This section presents the results findings for assessing security actions for improving the security of IS; challenges/incidents affecting IS; security maturity level of IS in organizations; security maturity comparisons in security domains across organizations, a case study of the education sector in Tanzania.

4.4.1 Security Actions for Improving Security of Information Systems

In addition to the survey questionnaire and semi-structured interview, the study employed a desk document review to find out how IS can be improved. This enabled triangulation in research methods, data collection and results findings for enhancing the security of IS, a case of the education sector in Tanzania. The results are as follows.

Semi-structured interview with a focused group: A study through a semi-structured interview with the focused group in regard to the question asked to respondents on "what do you think might be improved to increase information systems security in your organization?". Majority of respondents revealed that security awareness to top management in organizations should be conducted. This evidenced by responses during the interview from the organization L, K, O, M, P, N, and Q. The respondents

from organization L and Q pointed out that budget allocation is on ICT Development while the security of information systems is allocated a budget of 0% in most organizations in the education sector in Tanzania.

Desk document review: The study carried out a desk document review of some documents as summarized in Table 4.139. The study revealed that most organizations have ICT policies which have not been operationalized (left in draw i.e. locked in cabinets). Moreover, the study revealed that most organizations have security policies which have not been operationalized and some of them have partially operationalized security policies such as organization M (Table 4.139). Security awareness should be conducted for all employees and management.

Table 4.139: Desk Document Review

S/N	Document reviewed	Remarks	Findings
1	ICT policies	Desk document review was carried out for ICT policies for seven organizations under study	Most organizations have ICT policies which have not been operationalized.
2	Security Policies and operational manuals for IS	Desk document review was carried out for IT security policies and operational manuals for seven organizations under study.	It was revealed that most organizations have created security policies but not operationalized. Some of them have tried to operationalized part of security policy such as organization M.

The documents are not operationalized or partially operationalized due to the lack of ICT security budget for operationalising. Additionally, this is due to lack or ad-hoc security awareness training in most organisations. Thus organisations should allocate budget for security awareness training, and education; for operationalisation of security policies.

4.4.2 Challenges and Security Incidents Affecting Information Systems

The data were gathered through semi-structured interviews with a focused group (subject matter experts) and document review. Table 4.140 depicts the research findings on the response to the question asked during a semi-structured interview with a focused group on "challenges encountered and security incidents occurred in the given organization in the last 5 years to date". The interview results were coded, content analysis was applied to identify patterns and themes in regard to research questions.

The findings revealed that the existing online IS and e-services are faced with various challenges, incidents such as hacking of IS; computer viruses; theft of computers, laptops in the office and theft of laptops during travels. Furthermore, the study revealed that IS are faced with challenges of information resources capacity limit such as web server capacity limit, LAN, WAN or Internet bandwidth limit capacity; hardware or software failures; fire; floods; developing applications using code generators frameworks, open sources software or content management systems (CMS) such Joomla without shutdown open holes (vulnerabilities).

Table 4.140: Challenges, Incidents Affecting Information Systems/E-Services

S/N	Challenges/ Incidents	Implications	Organisation
1	Organisation O website & online application system was hacked on 2015-04-27:00:23	Denied access to services	Organisation O
2	Web Server limit: capacity	Denied access to services	Organisation P
3	Online IS/websites created using code generation frameworks/Open sources software or Content Management Systems (CMS) such Joomla without shutdown open holes; use of open	Vulnerability exploitation	Majority of organizations
4	Organisation P website was hacked on 2015-07-31: 16:50	Customers denied access to services.	Organisation P

S/N	Challenges/ Incidents	Implications	Organisation
5	Organisation L website and central admission system was hacked on July 2014	Customers denied access to services.	Organisation L
6	-Organisation M website was hacked on 2015-01-21:12:13; -Organisation M online application system; part: www.xxxxx/xampp/lang.tmp) was hacked	-The website was down for a few minutes and organization M restored back. -Hacking involved exploitation of vulnerabilities in xampp software which was installed on the server to run the online application system.	Organisation M
7	- Organisation K: Foreign award assessment system was hacked on 2015/09/29:14:35; - Organisation K website was hacked on 29/04/2011; 14/08/2012	Customers denied access to services.	Organisation K
8	Incorrect configuration of IS	Data inconsistencies.	Organisation M
9	Computer Viruses	Files and systems were affected	All 7 organizations under study
10	Theft of computers/ laptops in the office and theft of laptops during travels.	Loss of data and loss of confidentiality of information	All 7 organizations under study
11	Hardware/software failure:	Services were unavailable.	Organisation N
12	Fire	Information Resources and services interruptions	Organisation P
13	Flood in ground floors	Computing devices were affected.	Organisation K
14	Power fluctuation/ unavailability; AC failure in computing devices such as server rooms.	Customers denied access to services.	All 7 organizations under study
15	LAN/WAN unavailability; limited bandwidth	Customers denied access to services.	All 7 organizations under study

The research findings revealed that most organisations websites/e-services have been hacked in the period of 2011-2017 due to failure to incorporate security requirements during SDLC and lack or inequated security awareness training in most organisations. Organisation O website & online application system was hacked on 2015-04-27:00:23. Organisation P website was hacked on 2015-07-31: 16:50. Organisation L website and central admission system were hacked in July 2014. Organisation M website was hacked on 2015-01-21:12:13. Organisation K website was hacked on 29/04/2011; 14/08/2012; Organisation K: Foreign award assessment system was hacked on 2015/09/29:14:35. The hacking is due to misconfigurations of IS and

faliure to incorporate security requirements in every stage in SDLC; this leads to security holes (vulnerabilities) which are exploited by hackers. Thus, for enhancing the security of IS, organizations should conduct security awareness training and education to ICT staff. Security awareness training should be conducted for all employees and management.

4.4.3 Institutional Maturity Comparisons

This section presents the institutional maturity level comparison for seven organizations under study. The study found that information security maturity across organizations is 1 in SSE-CMM rating scale of 0-5 (Figure 4.1). It revealed that five organizations (L, O, M, N, and Q) out of seven have reached the education sector maturity level of 1; and the two organizations (K and P) are below the maturity level of 1. Thus, the study revealed that security controls and security measures are either lacking (scale 0: non-existent) or implemented in ad-hoc (scale 1: unplanned) manner in SSE-CMM rating scale of 0-5 (Figure 4.1). Thus, the security of information during capturing, storage, processing, and transmission in IS is questionable. For improving security, organizations should implement security controls and security measures for ensuring security goals (confidentiality, integrity, and availability) are achieved.

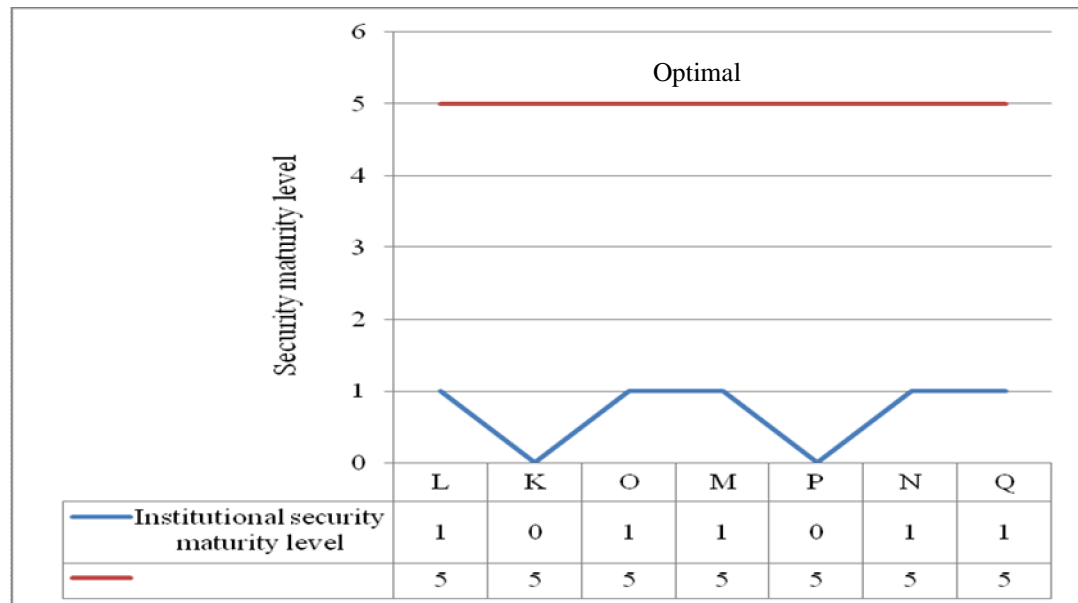


Figure 4.1: Institutional Maturity Level in SSE-CMM

4.4.4 Security Domains Maturity Comparisons

This section presents the maturity level analysis across information security domains for seven organizations under study. This enabled to ascertain the security status quo gap required for improvement and taking action to improve the situation. Security of IS was viewed as multi-layers of security with controls in each layer (domain). Table 4.141 depicts a list of security domains analyzed for security maturity level. The analysis was done in each security domain to determine the maturity level across the security domain, a case study of the education sector in Tanzania.

Table 4.141: Summary of Security Domain Assessed for the Maturity Level

Code	Security domain
ISO4	Risk management
ISO5	Security policy
ISO6	Organisational of information security
ISO7	Human resources security
ISO8	Asset management
ISO9	Access controls

Code	Security domain
ISO10	Cryptography
ISO11	Physical and environmental security
ISO12	Operations security
ISO13	Communication security
ISO14	Systems acquisition, development, and maintenance
ISO15	Supplier relationships
ISO16	Information security incidents management
ISO17	Business continuity
ISO18	Compliance

Table 4.142 presents the summary of findings for domain security analyzed in addressing the research question on how can the security of information during capturing, processing, storage, and transmission be improved in IS. The study depicts that security maturity level across security domain is 1 in SSE-CMM rating scale 0-5. The finding shows that the implementation of security controls for most security domains are performed in ad-hoc (performed informally). Thus, improving the security of IS, organizations should implement security controls for each security domain.

Table 4.142: Security Domains Maturity Level

Security domain	Organization							Security maturity domain level
	L	K	O	M	P	N	Q	
ISO4	1	0	3	3	0	1	0	1
ISO5	0	0	1	1	0	1	0	0
ISO6	0	0	1	1	0	1	1	1
ISO7	1	1	1	1	1	1	1	1
ISO8	1	0	1	1	0	1	1	1

Security domain	Organization							Security maturity
	1	1	1	1	0	1	1	
ISO9	1	1	1	1	0	1	1	1
ISO10	0	0	0	1	0	0	0	0
ISO11	1	1	1	1	1	1	1	1
ISO12	1	0	1	1	0	1	1	1
ISO13	1	0	1	1	0	1	1	1
ISO14	1	0	1	1	0	1	1	1
ISO15	1	1	1	1	0	1	1	1
ISO16	0	0	0	1	1	0	1	0
ISO17	1	0	0	0	1	0	0	0
ISO18	1	1	1	1	0	0	1	1
Institutional security maturity level	1	0	1	1	0	1	1	1

Source: Field data, 2020

The collected data were visualized using the timeline series graph to portray maturity level across the security domain, a case study of the education sector in Tanzania. From the graph (Figure 4.2), the study portrays that maturity level across domain is 1 in SSE-CMM rating scale 0-5. The study found that maturity level across security domains is a time series graph with a curve line having a maturity between 0 and 1 in SSE-CMM rating scale 0-5. For improving the security of IS, organizations should implement security controls/countermeasures for each security domain.

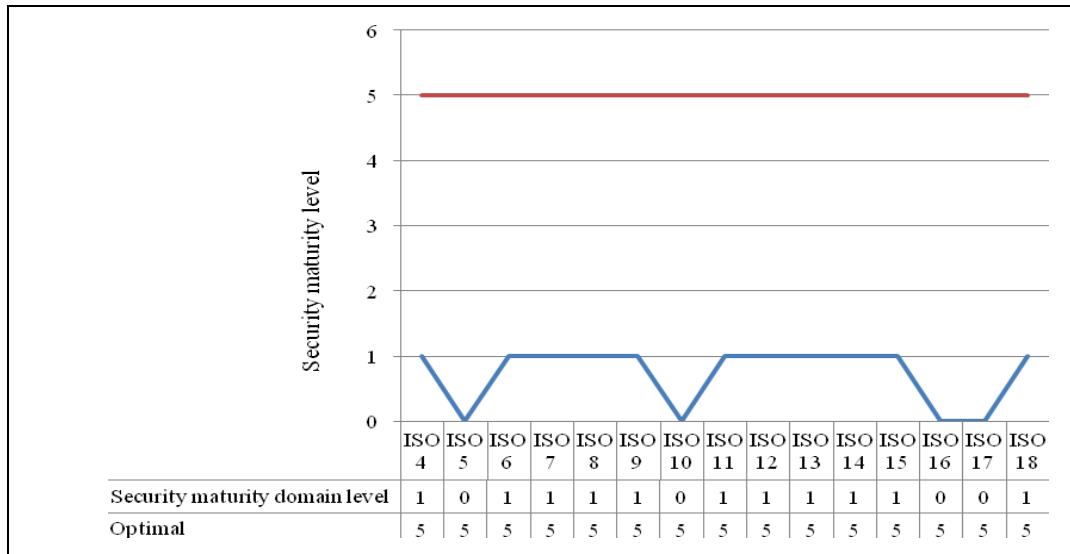


Figure 4.2: Line Graph For Security Domain Maturity Level

Further analysis was done using radar/ spider chart analytical tool; the choice of radar analytical tool was based on the nature of research question which involved multivariate observations sharing similar characteristics (security maturity levels in SSE-CMM rating scale of 0-5). The radar chart was used to visualize multivariate observations for institutional maturity level across security requirements domains.

Figure 4.3 depicts a radar chart for institutional security maturity across security domains. The radar shows that the security domain maturity is similar across security domains centred within radii of 1 in SSE-CMM rating scale of 0-5 radii. Further, the study found that the highest radius is 3 under risk management (ISO4) for organization M; most organizations have radii of 1 in SSE-CMM rating scale 0-5. For improving IS security, organizations should view security as a system with multi-layers security composed of different security domains interrelated to each other (Figure 4.3).

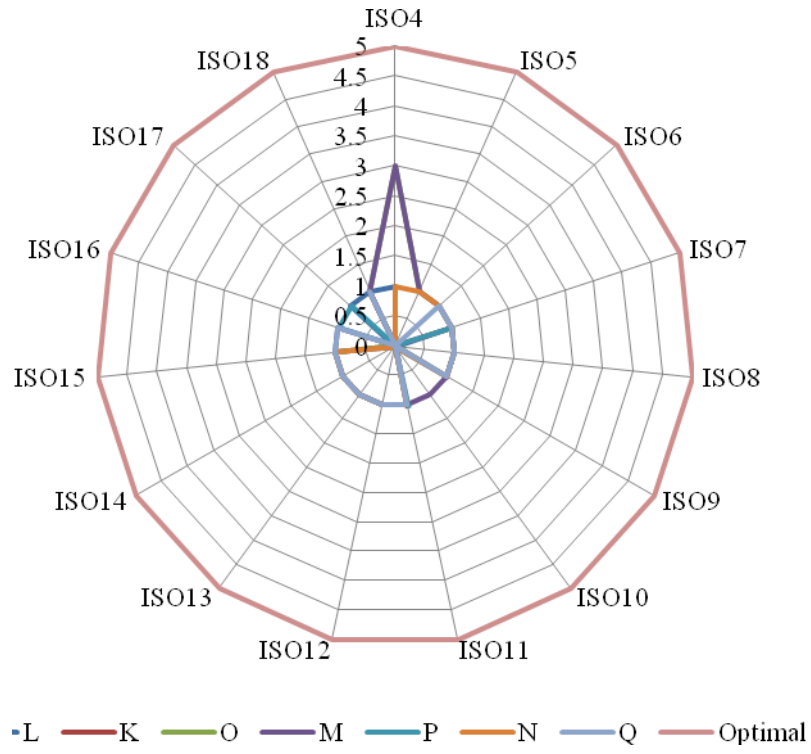


Figure 4.3: Radar for Institution Security Domain Maturity

CHAPTER FIVE

DISCUSSION OF THE FINDINGS

5.1 Introduction

This chapter presents the discussion of research findings. It presents a discussion on security measures. It presents security controls for ensuring security goals of information in information systems. It presents a discussion on how information systems security can be improved using a multi-layered security approach. It presents a framework for enhancing security of IS. It presents a prototype: Human sensor web prototype for crowdsourcing security incidents. It presents a Validation of the developed framework for enhancing security of information systems using cryptography based algorithm based techniques. It presents an evaluation of the developed framework. Lastly, it presents a discussion on the evaluation of the proposed Framework. The discussion is as follows.

5.2 Security Measures for Ensuring Security Goals

This section presents a discussion on security measures for ensuring security goals (confidentiality, integrity and availability) of information in IS during information states. It addresses the research question, RQ₁: To what extents are the existing security measures ensure confidentiality, integrity and availability of information in IS? The study was carried out to assess the existing security measures for ensuring confidentiality, integrity, and availability of information in IS. The investigation was based on SSE-CMM with a rating scale of 0-5. The study found that security measures for ensuring confidentiality, integrity, and availability are lacking or implemented in ad-hoc as depicted by research findings in section 4.2. The discussion for security measures for ensuring the confidentiality, integrity and

availability of information during information states is as follows.

5.2.1 Security Measures for Ensuring Confidentiality of Information

This section addresses the research question one, RQ1. The security measures for ensuring the confidentiality of the information in IS have been assessed (Section 4.2.1) and been summarized in Table 5.1. The study found that security measures for ensuring the confidentiality of the information in IS have been implemented in an ad-hoc manner (Section 4.2.1). Ensuring the confidentiality of the information in IS; it involves employing effective security measures (actions or procedures) to protect the information in IS against unauthorised/illegal access/view, disclosure/observation of information during capturing, processing, storage, and transmission of information. It includes technical and non-technical security measures. The following is the discussion on ensuring the confidentiality of the information in IS by employing effective security measures.

One of the security measures for ensuring the confidentiality of the information in IS; is designing and implementing effective identification, and authentication of accessing information in IS. The main concern in security is to bind the user to a given identity and use that identity as a means of granting or denying access to IT resources (IT assets). Identification is the process of uniquely identifying an identity of a user or process or system or application and binding it. Authentication is concerned with proving identity or claim of a user or systems or application or process is genuinely who claims to be through that identity presented for against the given claim.

The IS in cyberspace have been hacked due to the poor authentication practices either using the normal user ID and weak passwords or defaults ones. The study recommends using multifactor authentication. Figure 5.1 depicts proposed multifactor authentication system architecture for enhancing the security of information systems.

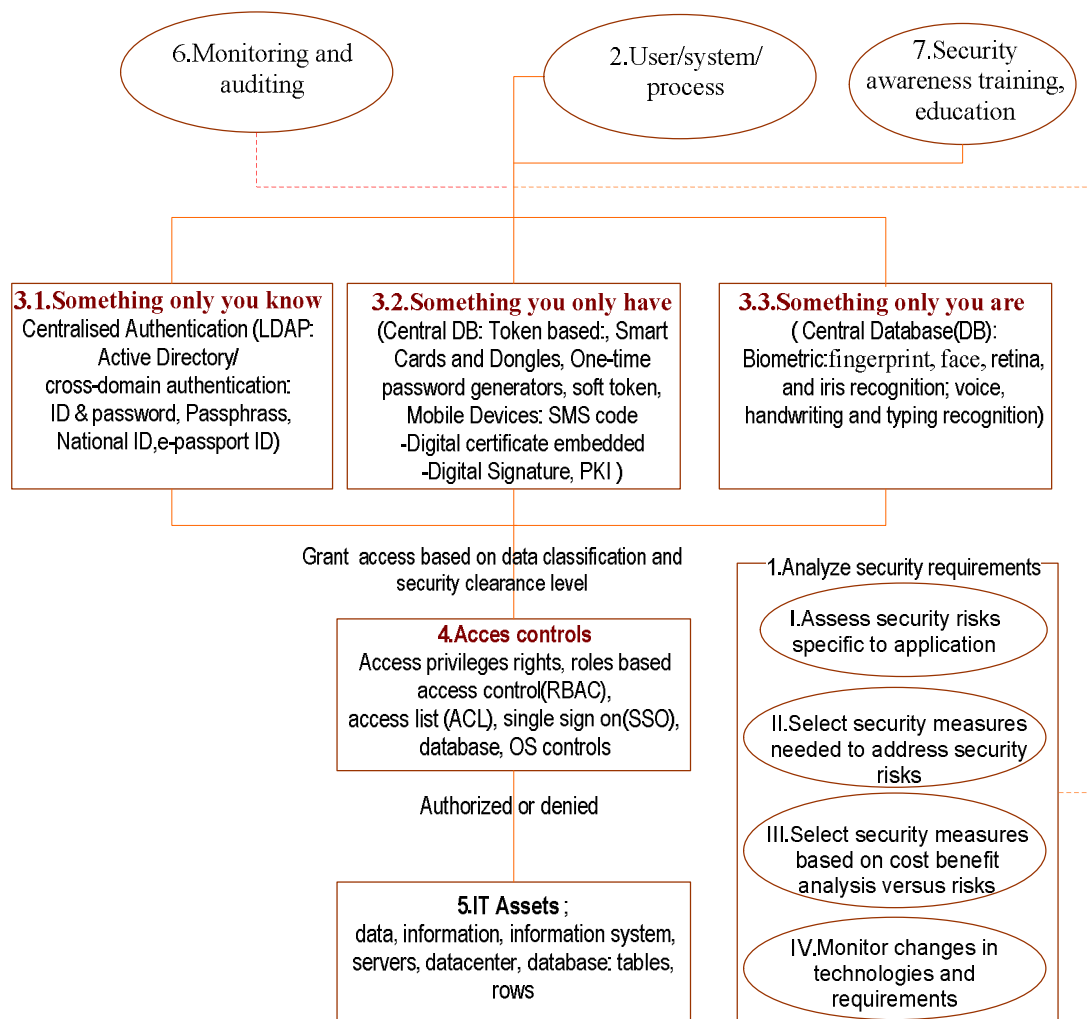


Figure 5.1: Proposed Authentication and Authorization System Architecture

The proposed authentication and authorization systems architecture, Figure 5.1, comprises of analysis security requirements, actor (user or system or process), authentication categories, access controls, IT assets to be protected, security awareness training, and education, and monitoring and auditing. The descriptions are

as follows.

(a) *Analysis of security requirements*

- i). First, assess security risks specific due to security concerns for information system components (applications, databases, network infrastructure, operating systems, people, and business process). Develop system architecture showing actors (or users), data/information flows for input and outputs. Perform data security classification of those data/information based on approved data/information classification scheme of the given organisation/sector (such as public, confidential, secret, top secret).
- ii). Second, select the effective security measures required to address security risks impacting the business.
- iii). Third, select security measures based on cost benefit analysis versus risks. Fourth, Monitor changes in technologies and requirement.

(b) Identification of user or system or process to be authenticated

The users or system process to be authenticated should be identified and how should interact with the information system. This includes should include defining the inputs and outputs to the actor (user or system or process) to be authenticated.

(c) Authentication categories

The authentication of the user to an information system involves three categories.

- i). First, something only you know (password, PIN, pass phrase and ID, National ID; based on centralised authentication (Active Directory/LDAP, cross-domain authentication).

- ii). Second, something you only have. This includes a token: Smart Cards and Dongles, soft token; one-time password (OTP) generators, mobile devices: SMS code. The token should be embedded with keys, digital certificate, digital signature and public key infrastructure (PKI). The study recommends the use of a centralised database from a trusted source to avoid unnecessary redundancies of storing the same identification and authentication data on multiple locations.
- iii). Third, something only you are (static biometric: fingerprint, face, retina, and iris recognition; dynamic biometric: voice, handwriting and typing recognition). The authentication should involve a combination of at least two categories forming multifactor authentication. For example, authentication using a user ID with pass phrase and code send to Mobile Devices via SMS.

(d) Access controls

After successful authentication of user; what follows is to ensure that the authenticated user has the access right to only required IT resources (IT assets). This should be based on the least privileges principles and need to know basis. The accesses rights can involve read, write, and execute (rwx on a UNIX system). Access controls determine which users are authorized to read, modify, add, view/select, insert, and delete information resources. It includes the use of access privileges rights; roles-based access control (RBAC), access control list (ACL), and single sign on (SSO) for authorization to IT assets.

(e) IT assets to be protected

The IT assets to be protected should be identified (create or update inventory list of IT assets). The IT assets should be classified and security protection requirements

should be identified for each IT assets. This includes access controls to protect data, information, information system, servers, datacenter, and database: tables, rows.

(f) Monitoring and auditing

Perform monitoring logs(Operating systems logs, database logs, application logs) and auditing for compliance of security measures implemented to if are implemented correctly as required (check audit trail for violation; you can do penetration testing/compliance audit testing)

(g) Security awareness training and education

Authentication should be accompanied with consistent awareness, education, and Training to all users of IS, management and to all ICT staff responsible for the day to day operations of IS. The study found that there is a lack of information security awareness training and education (section 4.2.1.8). Loss of confidentiality of the information has been mostly attributed to insider attacks(Symantec, 2019). The insider (user as users, IT administrators) attacks are mainly due to unaware users/employees who commit cyber crime internationally or unintentionally. Thus, for ensuring the confidentiality of information, organizations should conduct information security awareness training for all individuals interacting with IS. Conduct specialized IT security training to IT staff (programmers, systems/network administrators) and top management. This empowers them with necessarily security skills the problem of misconfiguration of IS and insecure coding for applications/programs. The security awareness to top management assists in gaining support for budget allocation for IT security and effective implementation of information security policy of the given organization.

For ensuring the confidentiality of the information in IS; authentication, access control and security awareness should be used in combination with other security measures as summarized in Table 5.1. The encryption is one of the security measures for ensuring the confidentiality of the information in IS during capturing, processing, storage and transmission of information. The encrypted data are vulnerable to cryptanalysis attacks (Kessler, 2019) for weak encryption algorithms with small key sizes. The higher key size the stronger the security of encrypted data/information during capturing, processing, storage and transmission in IS.

Figure 5.2 depicts a crypto system architecture for ensuring confidentiality of the information in IS during capturing, processing, storage and transmission of information. Confidentiality of information in IS during transmission and storage can be achieved as follows.

Confidentiality information in IS during transmission of information:

- i). Security requirement: ensure confidentiality of information during transmission; using asymmetric RSA algorithm with 1024 key size
- ii). Generate private key ($private_{ks}$) and public key ($public_{ks}$)
- iii). Encryption during transmission: sender prepares plaintext message m
- iv). The sender encrypts the plaintext message m using the public key, pub_{kr} of the receiver; $Encr_K(m_i, pub_{kr})$; the output $ciphertext = c_i$ is sent to a receiver
- v). The receiver, decrypt the $ciphertext = c_i$ using his/her private key of the receiver, $private_{kr}$; $Decrypt_k(c_i, private_{kr})$; output is Plaintext = m_i

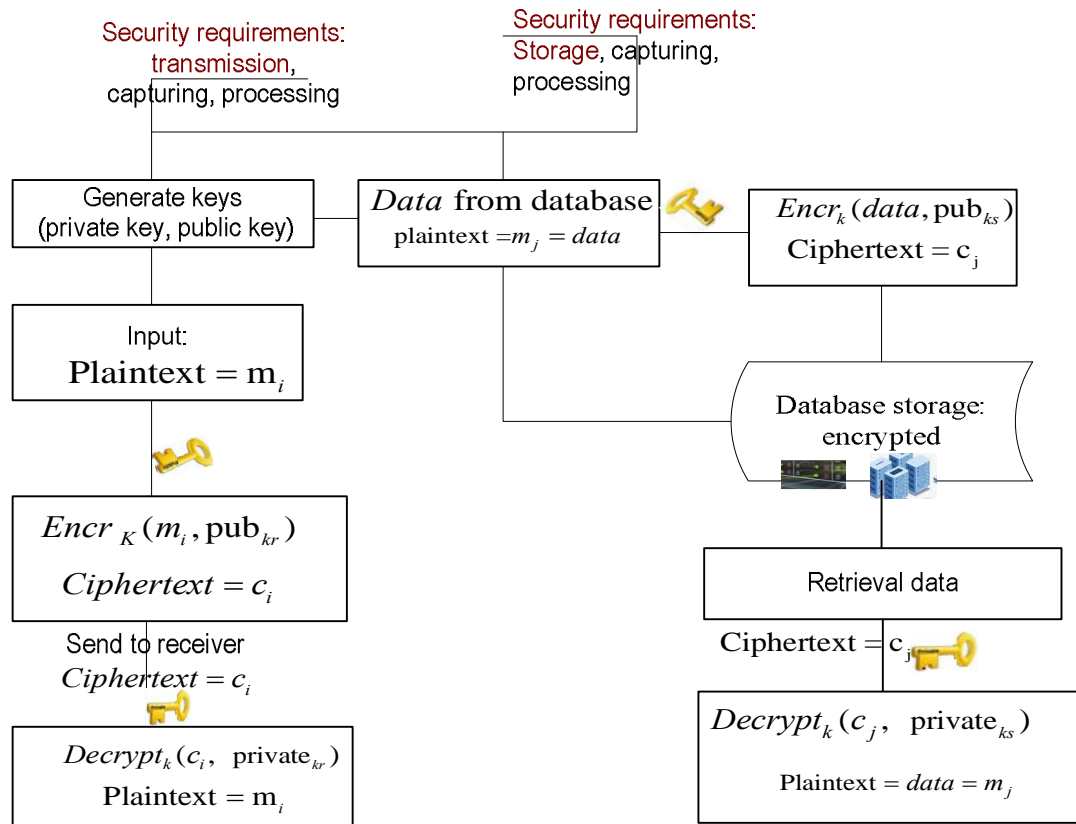


Figure 5.2: Crypto System Architecture for Ensuring Confidentiality of Information and Information Systems

Furthermore, from Figure 5.2, the confidentiality of the information in IS during storage can be ensured using encryption as follows:

Confidentiality of information in IS during storage of information in a database:

- i). Security requirement: ensure confidentiality of information during transmission; using asymmetric RSA algorithm with 1024 key size
- ii). The owner of the data generate/get private ($private_{ks}$) and public key(pub_{ks}) pair to be used for encryption
- iii). Retrieval and encrypt the plaintext = $m_j = data$ from the database using the public key pub_{ks} of data owner; $Encr_k(data, pub_{ks})$; output is ciphertext = c_j and stores the encrypted data, ciphertext = c_j in the database

- iv). Retrieving encrypted data; data owner retrieve encrypted data, ciphertext = c_j ;
 and decrypt using his/her private key; $Decrypt_k(c_j, private_{ks})$; output is
 $Plaintext = data = m_j$

For ensuring confidentiality of sensitive data stored in the cloud computing environment (untrusted third party), another form of encryption is employed, called homomorphic encryption (Gentry & Halevi, 2011; Acar et al., 2017); it allows processing encrypted data without decrypting them first (Acar et al., 2017). The study recommends the use of homomorphic encryption for ensuring the confidentiality of information captured, processed, stored and transmitted in the cloud ubiquitous computing environment. For ensuring the confidentiality of information captured, processed, stored and transmitted in IS in cyberspace the study recommends using strong algorithms with optimal performance large key size (AES algorithm for symmetric encryption with the key size 256 bits; RSA asymmetric encryption algorithm with key size 512 to 1024 bits).

Thus for ensuring the confidentiality of the information in IS; a combination of encryption with other security measures should be employed to form multi-layered security. The security measures for ensuring the confidentiality of the information in IS during capturing, processing, storage, and transmission of information in IS are summarized in Table 5.1. These are not an exclusive list for all security measures but are the commonly employed security measures for ensuring the confidentiality of the information in IS. It forms a template for security measures for ensuring the confidentiality of information. Others can be added to the list; like homomorphic

encryption for a cloud environment.

Table 5.1: Security measures for ensuring information states confidentiality

S/N	Security measures	Details	Information states			
			Capturing	Processing	Storage	Transmission
i.	Identification and authentication	Unique user account and password(something you know); security token such as smartcard (something you have); biometric (something your).	ç	ç	ç	ç
ii.	Access controls mechanisms	Classifying information, authorizing and revoking access rights; the use of technologies (firewalls, access control lists).	ç	ç	ç	ç
iii.	Network segmentation	Splitting a network into subnets, VLANs, physical separation of LANs.	ç	ç	ç	ç
iv.	Encryption of data/information	Encrypting sensitive data/ information.	ç	ç	ç	ç
v.	Media sanitization	Clearing, purging & destruction of data remanence prior disposal of media.	ç	ç	ç	ç
vi.	Disabling/blocking insecure services, protocols/ports.	Disabling/blocking insecure services, protocols/ports.	ç	ç	ç	ç
vii.	Patch management	Regular patching, updating of IS, hardware, operating systems, databases, anti-malware/antiviruses, ICT devices	ç	ç	ç	ç
viii.	Security awareness and training	Security awareness and training for non-disclosure of sensitive information.	ç	ç	ç	ç
ix.	Logging, monitoring of logs and alerting	Monitor logs for non-disclosure of sensitive information.	ç	ç	ç	ç

5.2.2 Security Measures for Ensuring the Integrity of Information

This section addresses part of the research question one, RQ1. The study found that security measures for ensuring the integrity of information in IS have been implemented in an ad-hoc manner (Section 4.2.2). Table 5.2 presents a summary of security measures for ensuring the integrity of information in IS. Ensuring data

integrity involves applying technical and non-technical security measures (actions, procedures) to safeguard against unauthorized modification or alteration of information in IS. The discussion of findings is as follows.

The researchers addressed the loss of integrity of information by employing technical and non-technical solutions. One of the technical techniques employed is cryptographic techniques. This includes a digital signature and hash function. A digital signature provides authentication (authenticity), integrity, and non-repudiation of the message (Kessler, 2019; Suhail et al., 2019). It uses asymmetric cryptography and hash functions algorithms. Digital signatures experience cyber-attacks such as protocol (such as exploit the malleability) cyber-attacks; mathematical; cryptanalysis cyber-attacks and side-channel cyber-attacks (Jang-Jaccard & Nepal, 2014). It should be employed in a multi-layered security approach. The study proposes cryptographic systems architecture for ensuring the integrity of information and information systems as presented in Figure 5.3. The digital signature is created by hashing the plaintext message and encrypting its hash value using a private key, $private_{ks}$ of the sender. It is verified using the public key of the sender, pub_{ks} .

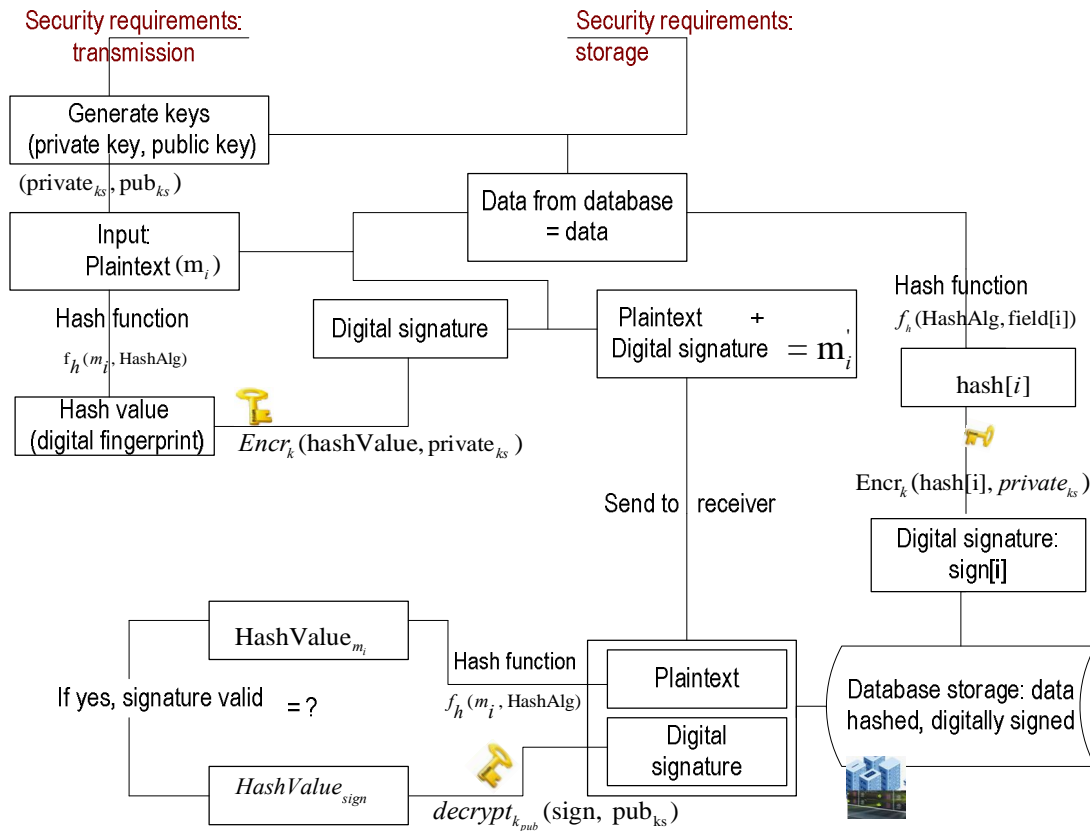


Figure 5.3: Cryptographic Systems Architecture for Enhancing the Integrity of Information And Information Systems

Digital signature additionally ensures authentication proof of the sender. Moreover, it guarantees non-repudiation of information during storage, processing and transmission. The sender cannot deny of creating a message and the receiver cannot deny has received the message. This should be based on the security requirements of information in IS.

From Figure 5.3, integrity during transmission can be ensured as follows.

- i. Select a strong cryptographic algorithm scheme for ensuring the integrity of information in IS during transmission in IS.
- ii. Generate the public key and private key pair represented by private_{ks} and pub_{ks}

respectively. Let m_i represent the input plaintext message space.

- iii. The plaintext m_i is hashed using a hash function, $f_h(m_i, \text{HashAlg})$ with effective hashing algorithm (HashAlg) such as SHA256. The output is a hash value (hash Value).
- iv. The hash value (digital fingerprint), hashValue is encrypted using a private key of the sender/data owner, private_{k_s} with function $\text{sig} = \text{Encr}_k(\text{hashValue}, \text{private}_{k_s})$. The sig is called the digital signature of the plaintext message m_i
- v. The digital signature is attached or appended to the original plaintext message m_i to form a digitally signed message $m'_i = (m_i, \text{sig})$.
- vi. The receiver retrieval the digitally signed message and compute the hash value of plaintext message m_i received, using a hashing function,

$$\text{hashValue}_{m_i} = f_h(m_i, \text{HashAlg}) \text{ with the same hashing algorithm.}$$

- vii. The receiver decrypts the digital signature, sig, using verification function $\text{decrypt}_{k_{pub}}$, $\text{hashValue}_{\text{sign}} = \text{decrypt}_{k_{pub}}(\text{sig}, \text{pub}_{k_s})$ to get a hash value,

$$\text{HashValue}_{\text{sign}} .$$

- viii. Verifying the digital signature, compare the two hash values in vi and vii ;

$$\text{hashValue}_{m_i} \stackrel{?}{=} \text{hashValue}_{\text{sign}} = \left\{ \begin{array}{l} \text{true, if the signature, sig, is valid} \\ \text{false, if the signature, sig, is invalid} \end{array} \right\}$$

- ix. If yes in viii the signature is valid, it means integrity, authentication (authenticity) and non-repudiation is guaranteed. If false the digital signature is invalid, reject the message as probably was tempered. Thus integrity,

authentication (authenticity) and non-repudiation cannot be guaranteed to the message m_i , communicate back.

Security requirements for ensuring integrity based on cryptographic techniques during storage as depicted in Figure 5.3, can be deduced as follows

- i. Determine security requirements of data/information for storing in the database based on security clearance and data/information classification level
- ii. Compute the hash value, $hash[i]$, using a hash function, $f_h(\text{HashAlg}, \text{field}[i])$ at field[i] based on the strong hashing algorithm, Hash Alg, such as SHA256
- iii. Sign data at column level: encrypt the hash value $hash[i]$ with a private key of the data owner using encryption function $\text{Encr}_k(\text{hash}[i], \text{private}_{ks})$; to get a digital signature, $sign[i]$ for field[i]
- iv. Verify the integrity of data by re-computing hash, $hash[i]_{m_i}$ at the given field[i] and comparing with the hash [i] value, $hash[i]_{sign}$ obtained after decrypting the digital signature, $sign[i]$ at the corresponding field[i].
- v. If the two hash values are equal, $hash[i]_{m_i} = hash[i]_{sign}$ then integrity, non-repudiations, authentication (authenticity,) is guaranteed during storage in IS. If the two computed hashes are not the same then data were changed during storage. Integrity, authenticity (authentication), non-repudiation, and cannot be guaranteed.

Digital signature be should employed in combination with other countermeasures such as message authentication codes (such as MACs, HMACs), audit trails, security awareness training and education and other security measures (as summarized in

Table 5.2). In securing web-applications IS are the application level, HMACs are employed in SSL/TLS protocols for ensuring integrity and authentication during transmission. Another security measure for ensuring the integrity of information is an audit trail.

An audit trail (also called the audit log) has been defined as a series of records of computer events, about an operating system, an application, or user activities. The findings revealed that most organizations have implemented an audit trail in ad-hoc for their sensitive IS (Section 4.2.2.8). Organizations should implement an audit trail (audit log) for a given sensitive information system and it should be periodically monitored. Audit logs monitoring includes application logs, database logs and server logs. The audit trails should be complemented by non-technical security measures such as security awareness training and education. The security awareness should be conducted to all users of IS and ICT staff who support the IS. Technical security measures can be passed due to social engineering, SQL injection flaws and cross siting script (OWASP, 2017). The security measures for ensuring the integrity of information in IS during information states (capturing, processing, storage, and transmission) in IS are summarized in Table 5.2.

Table 5.2: Security measures for ensuring the integrity of the information

S/N	Security measures	Details	Information states			
			Capturing	Processing	Storage	Transmission
i.	Access control mechanisms	Implement access control mechanisms: selective restriction of access to a place or information resources such as audit logs and systems logs.	ç	ç	ç	ç
ii.	Digital signature	Implement a digital signature to validate the authenticity and integrity of a message, software or digital document	ç	ç	ç	ç
iii.	Checksum(or hash sum)	Implement checksum such as MD5/SHA3 to verify the integrity of data.	ç	ç	ç	ç
iv.	Rotation of duties principle	Practice job rotation to breaks up opportunities for collusion and fraudulent activities.	ç	ç	ç	ç
v.	Segregation of duties principle	Duties should be sufficiently segregated in a given organization to ensure the detection of unintentional or unauthorized modification of information	ç	ç	ç	ç
vi.	Change management for IS	Implement change management and those changes should be documented, communicated, authorized, tested, implemented, monitored and audited to ensure the integrity of information and IS.	ç	ç	ç	ç
vii.	Logging, monitoring and alerting	Implement automatically logging, monitoring and alerting of security-related activities regularly	ç	ç	ç	ç
viii.	Audit trail	Implement and monitor the audit trail (audit log) for a given sensitive IS	ç	ç	ç	ç
ix.	Monitoring of wired(LAN, WAN) and wireless networks	Continuously monitoring of LAN/WAN and wireless networks for unauthorized access.	ç	ç	ç	ç
x.	Integrity monitoring tools	Integrity monitoring tools for alerting for any unauthorized modification	ç	ç	ç	ç
xi.	Least privilege principle/Need to know the principle	Implement procedures for reviewing users' access regularly, and only needed privileges should be applied and documented.	ç	ç	ç	ç
xii.	Configuration management	Ensure correct configuration implementation for their IS and ICT devices	ç	ç	ç	ç
xiii.	Patch management	Regularly patch their applications, operating systems, and ICT devices	ç	ç	ç	ç

5.2.3 Security Measures for Ensuring the Availability of Information

This section addresses part of the research question one, RQ1. The study found that security measures for ensuring the availability of information in IS are implemented

in an ad-hoc manner (Section 4.2.3). Table 5.3 presents a summary of security measures for ensuring the availability of information in IS. Ensuring data availability involves applying technical and non-technical security measures to safeguard against the loss of availability of information in IS. The discussion of findings is as follows.

Security measures for ensuring availability should ensure IS are configured with correct settings to allow authorised users to gain authorized access to information and information resources (IT assets) such as databases, servers, IS, storages, information processing facilities (IPF). This involves allocating required resources such as bandwidth for handling network traffics; processors processing power allocation; configuration of IS, applications servers, web-servers, databases servers to allow optimal concurrent requests connections in real time. It should ensure efficient uninterrupted access to information resources (called objects) and IPF by preventing any denial of services (DoS) attacks whether intentionally or unintentionally.

Technical and non-technical security measures are designed and implemented to provide access to authorized access to information and IS with acceptable performance level and to quickly handle interruptions (incidents). It includes providing redundancies for duplicating information resources and IPF in economical minimum special ways to provide quick recovery of information in IS. It should provide reliable backup processes and backup strategies for taking backups and testing of backups. The security measures should be designed and implemented to prevent loss of data/information or corruption.

Availability requirements for recovering information in IS should be defined based on the required time objective (RTO) and required point objective (RPO) for the information in IS. RTO is concerned with the required time to recover information system. RPO is concerned with amount data an organization is can tolerate to lose. RPO and RTO determine backup strategies: replication, transaction dumps differential, full backups and incremental backups; frequency of backup; backup media types and retention period. Different IS will have different RTO and RPO requirements over a different operational period in the year.

The loss of availability of information in IS is attributed to hardware failure; misconfiguration of IS components; software/application errors; environmental and physical threats (heat, flooding, power loss). DoS/Distributed denial of services attacks (DDoS) is the most cause loss of availability of information in IS. Additionally, it can be due to external attackers or insider attacks (intentionally or unintentionally). Systems/network administrators misconfiguring IS components; users of IS can delete files; overutilising of IS components (it includes hardware and software); under allocation of information processing resources and IPF.

Various security measures should be designed and implemented as summarized in Table 5.4. These include correct configuration of IS components; using access controls effectively; monitoring performance and network traffics: monitor operating, application logs; employs intelligent firewall and router with correct configurations for preventing DoS/DDoS attacks. Moreover, security measures include using redundancies (RAID 5 or RAID 10) and fault tolerance; taking backups and testing

backups restore. Availability of information in IS other attributes include usability, accesibility and timeliness. Usability is concerned with the easy to use or learn.

Accesibility is concerned with IS being accessilble, i.e subjects can interact with the information resources. Timeliness is concerned with a prompt response or providing a low-latency response. Ensuring availability of information in IS hosted in cyberspace such Internet against DoS/DDoS attacks due to heavy web traffics users requests. The study proposes a high avaliability distributed systems architecture integrated with a content delivery network (CDN) as presented in Figure 5.4. CDN is a distributed systems architecture for delivering contents to users based on their geographic location by caching them on the first visit as shown in Figure 5.4. It redirects traffics to the nearest server to the user. It increases content availability and redundancy: withstand hardware failures; it improves the security of IS by mitigating DDoS of information ans IS.

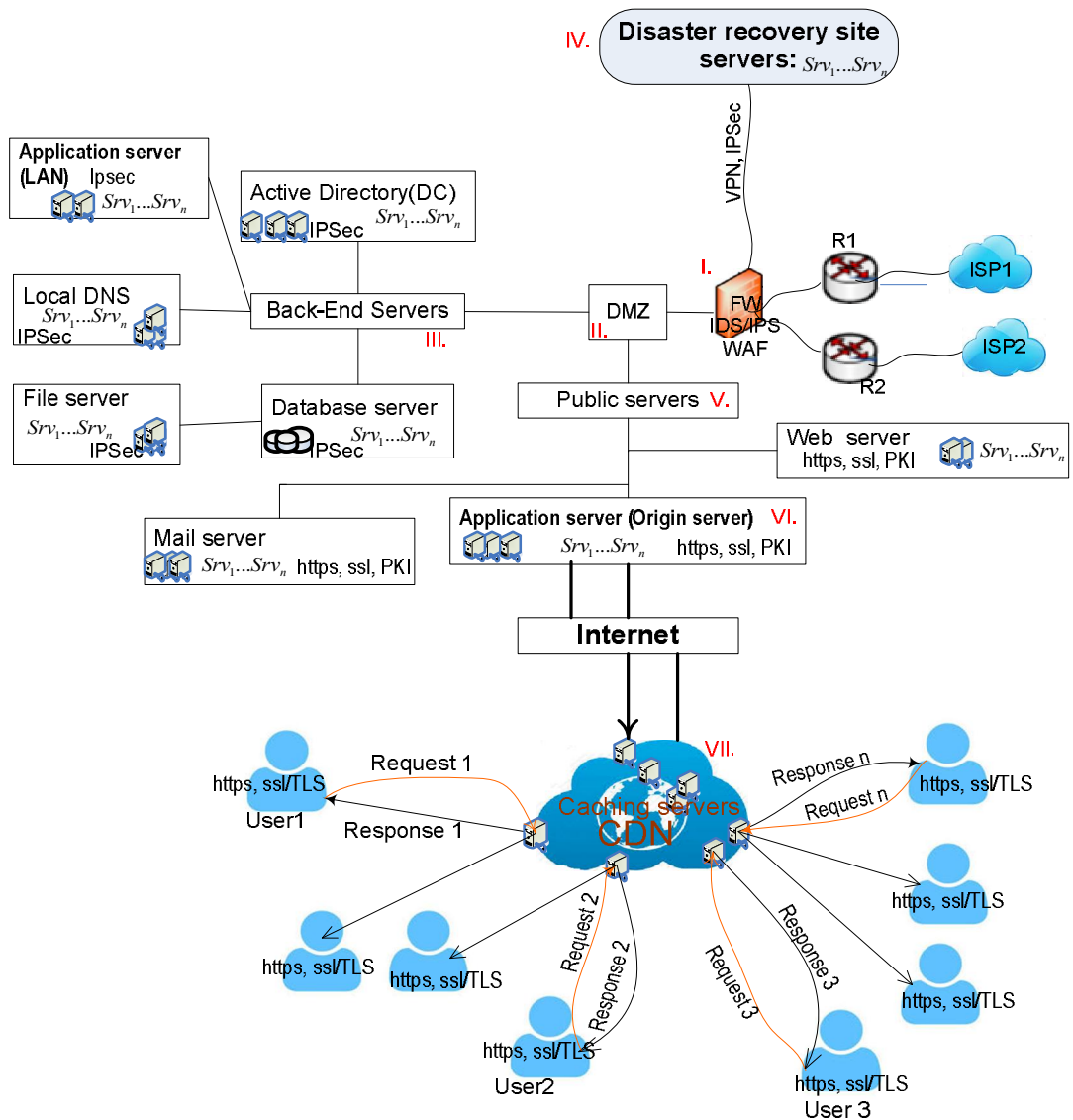


Figure 5:4: High Availability Distributed Systems Architected Integrated With CDN

From Figure 5.4, the following is the descriptions of the high availability distributed system architecture integrated with CDN.

- i. For high availability, two Internet services providers (ISP): ISP1 and ISP2 for providing loading balancing and redundancy in case one ISP fail. The firewall (FW) for filtering traffics and dropping protocols which are not allowed. It has intrusion detection (IDS) and intrusion prevention system

(IPS) for detecting malicious events and preventing them through IPS respectively. It includes a web application firewall (WAF) for protecting against common web-based attacks such as SQL injections.

- ii. Demilitarized (DMZ) zone is a network layer for protecting public accessible servers by assigning private IP and mapping with public IP addresses.
- iii. Back-end servers: are inside servers which accessible via LAN and need not be publically accessible on a public network such as the Internet; accessible from an untrusted public network using the virtual private network (VPN) such as IPsec site to site VPN or remote access SSL VPN.
- iv. Disaster recovery site: reliability is achieved through replicating data to offsite recovery site; in case of incidents affecting operations in the primary site business operations can continue from a disaster recovery site.
- v. Public servers are one accessible via the Internet, includes a web server, Mail server, and application server with an array of servers $Srv_1 \dots Srv_n$ for redundancy and load balancing of traffic requests and processing them.
- vi. The original server is the source of content for CDN; it contains the original contents of the users of IS. The content from origin server is cached by the edge servers and caching servers in the CDN.
- vii. CDN topology: consists of edge servers/caching servers. When the request is received, the edging server checks to see if the content requested is available in the cache and the cache has not expired, If not available or the cache has expired in the edge server, it requests that content to the origin server; then the response of content from origin server is cached in the edge server and response is given to the client. Cache server replicates the cached content

from the origin server to other servers in CDN topology. CDN topology in practice consists of farm array of servers from different datacentres distributed across the world continents.

From Figure 5.4, it is observed that clients/customer traffics are served from edge servers based on geographic locations in CDN. This results in using less bandwidth. It mitigates the risks of DoS/DDoS attacks contents have been cached in CDN from the origin server. Even if the origin server is attacked users/clients will continue to receive services from CDN. This CDN is mainly suitable for static contents from the origin server. In the education sector, CDN can be applied for the dissemination of students' exams results are accessible by more the 40 million people in Tanzania and across the world sending requests concurrently when results are announced. The request results in loss of availability of information in IS (result in DoS) and people fail to get exams results of students when are announced by the institution responsible for announcing exams students results in Tanzania. Also, for the dissemination of students' selection results to join form V schools and universities when are announced. Also, CDN can be employed for delivering e-Learning contents through online video; and online TV.

CDN should be employed in combination with other security measures for ensuring the availability of information in IS. It includes disaster recovery plan, business continuity plan, effective backup and periodic testing of backups and others security measures as summarized in Table 5.3.

Table 5.3: Security Measures for Ensuring The Availability of Information

S/N	Security measures	Details	Information states			
			Capturing	Processing	Storage	Transmission
i.	Business continuity plan	Implement BCP; document and test regularly the BCP; no insurance that operations ever be restored to their present state in case of disaster.	ç	ç	ç	ç
ii.	Incident management and response	Implement incident handling procedures; Functional incident response team and proper reporting.	ç	ç	ç	ç
iii.	Disaster recovery plan	Document; specify procedures to be followed in case of an event of a disaster.	ç	ç	ç	ç
iv.	Backup strategy	Implement backup strategies based on the required point objective (RPO): loss acceptable; and required time objective (RTO): the time required to restore IS to operation after disaster or emergency.	ç	ç	ç	ç
v.	Data backup process	The frequency of backup; labelling; retention period; the frequency of backup rotation.	ç	ç	ç	ç
vi.	Testing of the restore procedures	Test the restore procedures regularly.	ç	ç	ç	ç
vii.	Capacity planning	Predict and estimate the demand for information resources (IT assets).	ç	ç	ç	ç
viii.	Fault tolerance	Implement hardware and software redundancy; software recovery.	ç	ç	ç	ç
ix.	System monitoring mechanisms	Implement systems monitoring mechanisms.	ç	ç	ç	ç
x.	Protecting critical hardware and wiring from threats	Implement preventative measures to protect critical hardware and wiring from natural and man-made threats.	ç	ç	ç	ç
xi.	Change management for IS	Implement change management and those changes should be documented, communicated, authorized, tested, implemented, monitored and audited to ensure the integrity of information.	ç	ç	ç	ç
xii.	Patch management	Regularly patch the applications, operating systems, and ICT devices.	ç	ç	ç	ç
xiii.	Preventive maintenance	Regularly patching, updating antiviruses anti-malware, Operating systems.	ç	ç	ç	ç
xiv.	Configuration management	Ensure correct configuration implementation for the information systems and ICT devices.	ç	ç	ç	ç

5.3 Security Controls and Security Domains

This section presents a discussion on security controls and security domains for ensuring the security of information in IS. The study assessed the existing security

controls in IS (section 4.3). The investigation was based on SSE-CMM with a rating scale of 0-5(section 4.3). The research findings are presented in section 4.3. The research findings revealed that the existing security controls are not effective for ensuring security goals. The security controls were grouped into 15 domains namely: information security policy, organisational of information security, human resources security, asset management, access control, cryptography, physical and environmental security, operations security, communication security, systems acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, compliance, and risk management. The discussion of results in each security domain is as follows.

i). Information security policy

The security policy is essential for defining directions and responsibilities in ensuring the security of information in IS. The study found that are security policy in most organisations have been implemented ad-hoc manner or left in a draw without being operationalised. The study recommends that information security policy should be established, published and communicated to all relevant parties through security awareness training. It should be reviewed at a regular interval, every 3 years should be reviewed as technologies changes rapidly or reviewed as need arises even before the end of three years interval. The study recommends conducting security awareness to top management and IT staff. This is consistency with related studies (Bakari, 2007; Karokola, 2012; Shaaban, 2014; Carvalho & Marques, 2019; Tanovic & Marjanovic, 2019).

ii). Organisational of information security

The organisation of information security is concerned with controls in regard to the responsibilities and roles of security in the organisation. The study revealed that security responsibilities are not incorporated in job descriptions and duties and responsibilities of employees or suppliers or consultants interacting with the IT assets of the organisation (Section 4.3.2). The study found that a budget is not allocated for IT security. Additionally, it found that most organisations do not have individuals assigned security responsibilities at management posts and operations posts. The study recommends organisations should appoint a focal point person as a single contact for security management and implementation in the organization.

The study recommends security awareness to top management in regards to incorporating security responsibilities in all job description and duties; including signing non-disclosure agreement forms and security responsibilities to all employees and suppliers/consultants interacting with IT assets of the organization. Organisations should allocate budgets for enhancing the security of information in IS each year

iii). Human resources security

Human resources security is concerned with controls for minimizing risks from insider attacks (employees). The insider attackers contribute to most of cybercrimes attacks (Bosworth et al., 2014; Uctu et al., 2019) in organisations whether intentionally or accidentally. The study revealed that security awareness and education is performed in ad-hoc (Section 4.3.3). The study recommends that

security awareness programs should be conducted every 3 months (quarterly) per year, and this should be incorporated into organisation human resources capacity development policy.

iv). Asset management

Asset management is concerned with security controls for managing the security of assets. The study found that asset management has been implemented in an ad-hoc manner. The study recommends that information resources (IT assets) should be identified, classified in accordance with IT asset classification scheme (such as public, confidential, high confidential, secret, top secret). IT assets must have IT assets owner and who assign access privileges of users based on jobs responsibilities/duties. Furthermore, the study recommends a periodic review of IT asset classifications at least once per year. An organization should prepare and maintain a written inventory list of IT assets and should be evaluated every year.

The study, recommends organizations should label their data by indicating its confidentiality and criticality. A confidential label can be labelled public, limited access, restricted. Criticality label can be labelled as low; medium, high, very high. Security clearance for the classified information assets should be carried out based on a need to know background check.

v). Access control

This is concerned with access controls for ensuring the security of information in IS through granting and revoking access rights. The study found that access controls for managing granting and revoking access rights to users/system and password management are implemented in ad-hoc (Section 4.3.5). An

organisation should establish and implement an access control policy. The study recommends using role-based access and centralised access (Lightweight Directory Access Protocol (LDAP) and SSO or LDAP and Public key infrastructure (PKI)). This eliminates the risks of users sharing passwords and writing it down on files/desks or notebook. User accounts should be reviewed frequently (at least on a weekly basis) by using automated tools and manually by responsible staff. A user account should be revoked immediately when an employee's contract terminates/change jobs.

vi). Cryptography

Cryptography controls are concerned with ensuring proper and effective use of cryptography techniques to protect the confidentiality, authenticity or integrity of information. The study found that there is a lack of effective implementation of cryptographic controls (Section 4.3.6). The study recommends that organizations should establish policy and guidelines for the use of cryptographic techniques for ensuring confidentiality, integrity, authenticity, non-repudiation of information. This should include identifying cryptographic standards algorithms which include hash functions and encryption algorithms (asymmetric and symmetric encryption).

Security awareness should be conducted to management in regard to the use of cryptographic techniques for ensuring security. Security training and education should be conducted to ICT staff on the use of cryptographic techniques. This is consistent with other studies in the literature (Karokola, 2012; Shaaban, 2014; Carvalho & Marques, 2019).

vii). Physical and environmental security

This is concerned with physical and environmental security controls to prevent the loss, damage, theft/compromise of IT assets and interruptions to organisations operations. The study found that physical and environment security controls have been implemented in an ad-hoc manner (Section 4.3.7). The study recommends that organisations should establish physical and environment security policy. Sensitive areas should be identified and more controls should be implemented such as logbook for recording who enter the sensitive areas; including security clearance before entering the sensitive area. For datacentre/server room the organisation should install a fire suppression sub-system; cooling sub-system; and monitoring sub-system.

Physical and environmental security extends to cloud computing and virtualisation technologies. An organisation should have an inventory of all services hosted in the cloud; including virtual machines hosted in the organisation physical servers. An organisation must establish security controls for safeguarding IT assets in the cloud which can include virtual servers and storage spaces. The study recommends the use of homomorphic cryptograph for securing data in the cloud computing environment. It allows processing encrypted data without a need for decrypting them first (Acar et al., 2017).

viii). Operations security

The study found that operation security controls have been implemented in ad-hoc (Section 4.3.8). An operation security policy needs to be established and operationalised. Acceptable usage policy (UAP) as part of operation security

should be established. UAP contains the do and doesn't, and best practices for IT resources usage. The organisation should conduct security awareness in regard to UAP to all employees. Every employee should be given UAP and every employee should sign compliance with it. There should be a separation of testing, development and production environment.

Organizations should implement controls for automatic recording and monitoring of logs to ensure accountability of operation activities. The study recommends the use of an automated centralised log management system for OS, LAN, databases and applications. Organisations should implement automatic procedures for detecting, preventing and eradicating malicious codes. This includes the use of antiviruses, intrusion detection system (IDS) and intrusion prevention system (IPS). This is consistency with other studies in the literature (Aissaoui et al., 2017; Agrawal et al., 2018; Burton & Straub, 2019).

ix). Communication security

The findings in section 4.3.9 revealed that communication security controls have been weakly (ad-hoc) implemented in most of the organisations. The study recommends the implementation of network security management controls for protecting the information in the network. The network should be segmented by grouping related services, user department functions/services. Techniques can involve creating a virtual LAN (VLAN) for every department users or units. The organisations should establish and operationalise policies and procedure for information transfer in the network. Set appropriate procedures for agreements and information transfers. This should include electronic messaging and non-

disclosure agreements based on information classification scheme. The electronic transaction policy and procedures should in compliance with international standards and Tanzania transaction Act 2015(URT, 2015b) This is consistence with other studies in the literature (Beissel, 2014; Mahundu, 2016; Rizk et al., 2019).

x). Systems acquisition, Development and maintenance

The findings in Section 4.3.10 showed that acquisition, development and maintenances controls are either lacking or implemented in ad-hock. Most organisations develop software/applications without incorporating security requirements during SDLC such as validation checks, systems testing and user accepting testing. Failure to incorporate security requirements in SDLC is the causes of most cyber-attacks (Nfuka *et al.*, 2014; Mshangi, *et al.*, 2016; Symantec, 2019).

Open holes/ vulnerabilities are introduced due to misconfiguration and insecure coding. This results in loss of confidentiality, integrity and availability of information in IS. The study recommends organizations should establish and operationalise secure development policy and procedures by incorporating secure system engineering principles in every stage of SDLC. Organizations should provide secure coding training to ICT staff (systems analysts, programmers, administrators, IT security officers). This is consistence with other studies in the literature (Baset & Denning, 2017; OWASP, 2017; Wang et al., 2018).

xi). Supplier relationships

The findings results in Section 4.3.11 revealed that most organisations do implement supplier relationship management controls in ad-hoc (unplanned). Organisations should establish and operationalise supplier relationship policies and procedures. It includes establishing all relevant security requirements and agreeing with each supplier that may capture, process, store, communicate/provide ICT infrastructure for the organisation information in IS. A supplier should sign non-disclosure agreements and acceptable data use.

Moreover, screening/background check and security awareness training should be conducted to suppliersøstaff accessing information in IS. This should include risk an assessment for information in IS accessed by suppliers, and define and implement and agreed security requirements controls to mitigate the risks. This is consistence with other studies in the literature (Martínez et al., 2013; Shaaban, 2014; Tang et al., 2018; Rizk et al., 2019).

The findings in Section 4.3.12 showed that most organisations implement security controls for incidents managements in ad-hoc (unplanned). Organisations should establish effective incidents and improvement management policies, procedures and approaches for managing security incidents affecting IS. It includes establishing management procedures for quick enforcing effective response to information in IS security incidents.

The organisations should acquire resources/equipment needed for incidents handling and collecting digital evidence for forensics investigation. An

organisation should assign and train at least one staff for handling security incidents and for using tools to recover and examine data. The study recommends adoption of human sensor web crowd sourcing (Tsega et al., 2015; Kipanyula et al., 2016) for managing information in IS security incidents (Mshangi et al., 2018) at the sector level and across the country. The security incidents reported are analysed and response solutions for challenging incidents resolution should be awarded a prize like in crypto bitcoin chain. This is consistency with other studies in the literature (Rupere et al., 2012; ISACA, 2016; Tanovic & Marjanovic, 2019).

xii). Information security aspects of business continuity management

The findings in Section 4.3.12 revealed that most organisations inadequately implemented security controls for information security aspects of business continuity management and redundancies. Organizations should establish and operationalize business continuity management plan (BCMP). BCMP includes information security continuity and redundancies controls. The organization should establish business continuity requirements, document, implement and maintain processes, procedures and controls for ensuring the security requirement level of continuity for information security during disaster (crises/adverse) situations are met. Redundancy controls should be defined sufficiently to meet the availability of information processing facilities. The study recommends organizations should establish, operationalize and perform testing of a BCMP at regular intervals (at least twice per year). This ensures that the plan is valid and effective during a disaster. This is consistency with other studies in the literature (Gomes et al., 2017; Fernando, 2018).

xiii). Compliance

The findings in Section 4.3.12 revealed that most organisations do not conduct an assessment for compliance controls. Vulnerability assessment and penetration testing for IS are not carried out in most organisations. The study recommends compliance assessment for technical controls and compliance to policies (check compliance for information security policy) and standards to be carried out at regular interval (at least once per year). Vulnerability assessments should be carried out for a given information system/application during the testing phase of SDLC. It should be repeated when the given system is deployed in a production environment. Organizations should perform regular vulnerability assessments/penetration testing for IS in production at least twice per year. The identified vulnerabilities and risks during vulnerability assessments/penetration testing should be rectified to ensure security goals for information in IS. This is consistency with other studies in the literature (Beissel, 2014; Altaf et al., 2016; Jimenez, 2016; TCRA, 2017; Carvalho & Marques, 2019).

xiv). Risk management

The findings in Section 4.3.12 revealed that most organisations do not have a risk management program and risk register. Additionally, the study revealed that most organisations do not review and update risk register or they do in an ad-hoc manner. The study recommends that organisations should conduct IT risk assessments to identify likely hood and impact on the information in IS in regard to security goals (confidentiality, integrity, and availability) and business processes. Organizations should establish IT risk register based on IT risk assessments. The IT risk register should be reviewed and updated regularly (at every 3 years or when changes in

technologies or business processes). This is consistency with other studies in the literature (Ghotbi & Gharechehdaghi, 2012; NIST, 2012; Pan & Chen, 2012; Rizk et al., 2019; Uctu et al., 2019).

The study proposes a multi-layered security approach using SSM compounded with DSR. SMS integrated with DSR (termed as soft design science) was employed in the design of security controls for ensuring security goals for IT assets against security breaches (Mshangi et al., 2017). Based on the literature review and research findings; discussion of findings; and the security controls in each security domain are summarized in Table 5.4.

Table 5.4: Summary of Security Controls and Security Domains

S/N	Security domain	Security controls measures	The information states	Controls category				
				According to nature	Controls relative to the time			
					De	De	Pre	Co
i.	Information security policy	-Information Security Policy approved by the top executive or board of trustee; and operational. - Review of the policies for information security	Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç	ç
ii.	Organisational of information security	Chief Information Security Officer (CISO) or equivalent job responsibilities assigned.	Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç	ç
	(a).Internal organisation	Roles and responsibilities allocated to individuals		Administrative control	ç	ç	ç	ç
	(b).Mobile devices and teleworking	Policies and controls for mobile devices (such as laptops, tablet PCs, wearable)		Administrative control	ç	ç	ç	ç
iii.	Human resources security	Policy for human resources security in place.	Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç	ç
	(a).Prior to employment	-Screening -Terms and conditions of employment		Administrative control	ç	ç	ç	ç
	(b)During Employment	-Management responsibilities -Information security awareness, education, and training -Disciplinary process		Administrative control	ç	ç	ç	ç

S/N	Security domain	Security controls measures	The information states	Controls category				
				According to nature	Controls relative to the time			
					De	De	Pre	Co
	(c) Termination and change of employment	Termination or change of employment responsibilities		Administrative control	ç	ç	ç	ç
iv.	Asset management	Asset management Policy in place.		Administrative control	ç	ç	ç	ç
	(a).Responsibility for Assets	-Inventory of assets -Ownership of -Acceptable use of assets		Administrative control	ç	ç	ç	ç
	(b).Information classification	-Classification of information -Labelling of information -Handling of assets -Return on assets		Administrative control	ç	ç	ç	ç
	(c).Media handling	-Secure deletion -Destroying or degaussing physical media -Secure disposal or re-use of media -Physical media transfer		Technical control	ç	ç	ç	ç
v.	Access control	Access control policy in place.		Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç
	(a).Business requirements for access	-Clearly documented -Restrict network access and connections	Technical control		ç	ç	ç	ç
	(b).User access management	User registration and de-registration -Privilege management -Management of secret authentication information of users -Review of user access rights -Removal or adjustment of access rights	Technical control		ç	ç	ç	ç
	(c).User responsibilities	Use of secret authentication information to make users accountable for safeguarding their authentication information	Technical control		ç	ç	ç	ç
	d). System and application access control	-Information access restriction -Secure log-on procedures -Password management system -Use of privileged utility programs -Access control to program source code	Technical control		ç	ç	ç	ç
vi.	Cryptography	Cryptographic policy in place (to ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity).	Capturing, Processing, Storage, Transmission		Administrative control	ç	ç	ç

S/N	Security domain	Security controls measures	The information states	Controls category				
				According to nature	Controls relative to the time			
					De	De	Pre	Co
	(a).Cryptographic controls	-Policy on the use of cryptographic controls -Key management		Technical control	ç	ç	ç	ç
	(b).Encryption	Encryption of data/information		Technical control	ç	ç	ç	ç
	(c). Cryptographic authentication and integrity	-Digital signature; -Message authentication code (or cryptographic checksum)		Technical control	ç	ç	ç	ç
vii.	Physical and environmental security	Physical security policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç	ç
	(a).Secure area	-Securing offices, rooms and facilities. -Public access, delivery and loading areas; doors, lock, electric fence, CCTV, smartcard, biometric (e.g. fingerprint). -Physical security perimeter -Physical entry controls -Working in secure areas	Capturing, Processing, Storage, Transmission	Physical control	ç	ç	ç	ç
	(b).Protecting against external and environmental threats	-Protecting against fires, floods, earthquakes, bombs, etc. -Climate-protecting system, fire suppression system		Physical control	ç	ç	ç	ç
	(c).Equipment	-Equipment shall be correctly maintained to ensure its continued availability and integrity. -Equipment siting and protection -Supporting utilities -Cabling security -Equipment maintenance -Removal of assets -Security of equipment and assets off- premises -Security disposal or re-use of equipment -Unattended user equipment -Clear desk and clear screen policy		Physical control	ç	ç	ç	ç
viii.	Operations Security	Operations security policy in place	Capturing, Processing, Storage,	Administrative control	ç	ç	ç	ç

S/N	Security domain	Security controls measures	The information states	Controls category				
				According to nature	Controls relative to the time			
					De	De	Pre	Co
	(a).Operational Procedures and Responsibilities	-Documented operating procedures -Change management -Separation of development, test, and operational environments	Transmission	Administrative control	ç	ç	ç	ç
	(b).Protection from Malware	Controls against malware to ensure that information and information processing facilities are protected against malware		Technical controls	ç	ç	ç	ç
	(c).Back-Up	Information backup to protect against loss of data		Technical controls	ç	ç	ç	ç
	(d).Logging and monitoring to record events and generate evidence	-Event logging -Protection of log information -Administrator and operator logs -Clock Synchronization		Technical controls	ç	ç	ç	ç
	(e). Control of operational software	Installation of software on operational systems controls to ensure the integrity of operational systems		Technical controls	ç	ç	ç	ç
	(f). Technical Vulnerability Management	-Management of technical vulnerabilities -Restrictions on software installation		Technical controls	ç	ç	ç	ç
	(g). Information Systems Audit Considerations	Information systems audit controls to minimize the impact of audit activities on operational systems		Capturing, Processing, Storage, Transmission	Compliance control	ç	ç	ç
ix.	Communication security	Communications and operations policy in place.	Transmission	Administrative control	ç	ç	ç	ç
	(a).Network security management	-Networks and network services should be secured; -Network segmentation or segregation.		Technical control	ç	ç	ç	ç
	(b).Information transfer	Policies, procedures and agreements in place (confidentiality or non-disclosure agreements) for information transfer to/from third parties, including electronic messaging.		Administrative control	ç	ç	ç	ç
x.	System acquisition, development and maintenance	System acquisition, development and maintenance policy in place.	Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç	ç

S/N	Security domain	Security controls measures	The information states	Controls category				
				According to nature	Controls relative to the time			
					De	De	Pre	Co
	(a).Security requirements of information systems	-Security requirements analysis and specification -Securing applications services on public networks -Protecting application services transactions.		Administrative control	ç	ç	ç	ç
	(b).Security in development and support processes	-Secure development policy -Change control procedures - Technical review of applications after operating platform changes -Restrictions on changes to software packages -System development procedures -System security testing		Administrative control	ç	ç	ç	ç
	(c).Test data	Protection of test data controls to ensure the protection of data used for testing		Administrative control	ç	ç	ç	ç
xi.	Supplier relationships	Supplier relationships policy in place to ensure the protection of the organization's information that is accessible by suppliers	Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç	ç
	(a).Security in supplier relationship	-Information security policy for supplier relationships -Addressing security within supplier agreements -ICT Supply chain		Administrative control	ç	ç	ç	ç
	(b).Supplier service delivery management	-Monitoring and review of supplier services -Managing changes to supplier services		Administrative control	ç	ç	ç	ç
xii.	Information security incident management	Information security incident management policy in place.		Administrative control	ç	ç	ç	ç
xii(a)	Management of information security incidents and improvements	There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively, and to collect forensic evidence.	Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç	ç
xiii.	Business continuity	Business continuity plan document in place.	Capturing, Processing, Storage,	Administrative control	ç	ç	ç	ç

S/N	Security domain	Security controls measures	The information states	Controls category				
				According to nature	Controls relative to the time			
					De	De	Pre	Co
	(a).Information security aspects of business continuity management	-Planning information security continuity -Implementing information security continuity -Verify, review and evaluate information security continuity	Transmission	Administrative control	ç	ç	ç	ç
	(b). Redundancies	IT facilities should have sufficient redundancy to satisfy availability requirements.		Technical control	ç	ç	ç	ç
xiv.	Compliance	Compliance policy in place to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security	Capturing, Processing, Storage, Transmission	Administrative control	ç	ç	ç	ç
	(a).Compliance with legal and contractual requirements	The organization must identify and document its obligations to external authorities and other third parties in relation to information security.		Compliance control	ç	ç	ç	ç
	(b).Information security reviews	-Independent review of information security -Compliance with security policies and standards -Technical compliance review (IS vulnerability testing, penetration testing)		Compliance control	ç	ç	ç	ç
xv.	Risk Management	-Develop and operationalize risks register - Conducts routine risk assessments	Capturing, Processing, Storage, Transmission	Compliance control	ç	ç	ç	ç

5.4 Framework for Enhancing Security of Information Systems

This section presents the development process of the framework for enhancing the security of IS. The developed framework addresses the main research problem of the loss of confidentiality, integrity and availability of information in IS during information states (capturing, processing, storage and transmission in IS), a case study of the education sector in Tanzania. More this section presents a validation of

the framework for enhancing the security of information systems using cryptographic techniques. It develops an algorithm for enhanced security of IS based on cryptographic techniques. Furthermore, it develops its prototype for validating proof of concept based on cryptographic techniques.

5.4.1 Requirements for Developing Framework for Enhancing Security of Information Systems

Soft design science (SSM integrated with DSR) (Section 3.2) was employed in conjunction with a use case analysis technique to establish requirements for developing a framework for enhancing the security of information systems in systematic manner iterations until optimal was reached. The conceptual model was developed and compared with the real world (Section 2.7) to get feasible desirable change for taking action (Checkland, 1998) to improve the problem of failure to ensure security goals (confidentiality, integrity and availability).

Use case analysis (Vemuri et al., 2017) was employed to analyse requirements for the development of a framework for enhancing the security of information systems. The use case analysis was used to understand the interrelated components security requirements and its associated risks in IS as summarized in Table 5.5. These security requirements were gathered through a literature review (Chapter 2) and results findings (Chapter4). The security concern was identified in each component of the information system: hardware, software, database/data, networks, business processes/procedures, and people.

Table 5.5: Information Systems Components Descriptions and Associated Risks

S/N	Component	Description	Associated risks
1	Hardware	<ul style="list-style-type: none"> • It responsible for housing, storing, processing, transporting data/information and providing interfaces for capturing data/information. • Physicals security of hardware such as processor, RAM, hard disks should be ensured through physical security policy and other security controls 	<ul style="list-style-type: none"> • Physical hard disk failures, hardware malfunction; theft of hardware, electricals power disturbance such as brownouts, sags, & surges; static electricity shortage to hardware. • Natural hazards such as power failure, heat, humidity. It is affected by natural hazards such as water floods, heat, dirt and dust, radiation
2	Software	<ul style="list-style-type: none"> • It comprises of applications, operating systems (services such as file sharing, print sharing, client/server operations) • Security controls should be defined to ensure security goals (CIA triad) for software 	<ul style="list-style-type: none"> • Failure to update software, application software, results in open holes security vulnerabilities. • Buffer overflow caused by not limiting input data; this exceeds RAM buffer. It is due to poor programming practices. • Poor programming practices; without including security during SDLC, taken as an after thought
3	Data	<p>Data are stored in relational databases or files</p> <p>Data captured, processed, stored, and transmitted in IS must be protected to ensure security goals by incorporating security measures and security controls.</p>	<ul style="list-style-type: none"> • Data/database corruption, data inconsistence due to malicious attacks • Injection flaws: SQL injections, cross site scripts
5	Networks infrastructure	<p>Data/information are processed and transmitted over the networks infrastructure. Most IS are accessible via networked environment and hosted in cyberspace such cloud or locally hosted but accessible via the Internet.</p>	<ul style="list-style-type: none"> • Violation of confidentiality, integrity and availability for information during transmission in IS due to malicious attacks • Replays attacks; a man in the middle attacks due to malicious code attacks. • Single point of failure in network infrastructure without redundancy results in downtime • Unplanned capacity in terms of bandwidth; concurrent connection n lead to system unavailability • Malicious attacks to network infrastructure can result in DoS/DDoS attacks • Sessions hijacking and by pass authentication over the network.
6	Business processes/procedures	<ul style="list-style-type: none"> • It includes business processes/procedures: written instructions for operating a 	<ul style="list-style-type: none"> • Information systems deployed without proper defined business process or procedures can result in a violation of

S/N	Component	Description	Associated risks
		<p>given system employed to accomplish tasks.</p> <ul style="list-style-type: none"> • An organization should provide awareness of business processes/procedures to members of the organization only based on a need to know basis. 	<p>security goals.</p> <ul style="list-style-type: none"> • Failure to provide security awareness training, education on the protecting the procedures of operating IS can result in a violation of confidentiality, integrity and availability of information in IS.
7	People	<ul style="list-style-type: none"> • People are the weakest link in the security of IS; they can accidentally or intentionally damage or lose information/data • Security controls such as policy, education and security awareness and technical controls should be employed to protect against violation of security goals (CIA triad) due to actions of people 	<ul style="list-style-type: none"> • Social engineering attacks. • Lack of security awareness training and education results in loss confidentiality,

The information in IS exists in four states, namely capturing, processing, storage and transmission in IS for any given component of IS. Security requirements should be defined in each information states. Capturing states is always forgotten and results in IS which are vulnerable to cyber-attacks as security requirements in SDLC are considered as an afterthought. Thus, for ensuring the security of IS, security requirements should be incorporated in every stage of SDLC. The security requirements for developing a framework for enhancing security are summarized as follows.

- i. Security mechanisms for analysing and identifying security measures and security controls for enhancing the security of information in IS.
- ii. Identify security controls in each security domain for enhancing the security of information in IS
- iii. Design and implement effective security measures and security controls for ensuring security goals (confidentiality, integrity and availability) for

information during information states (capturing, processing, storage and transmission) in IS

- iv. Employ multi-layered security approach by incorporating effective security measures and security controls in each security domain for ensuring goals of information during information states (capturing, processing, storage and transmission) in IS

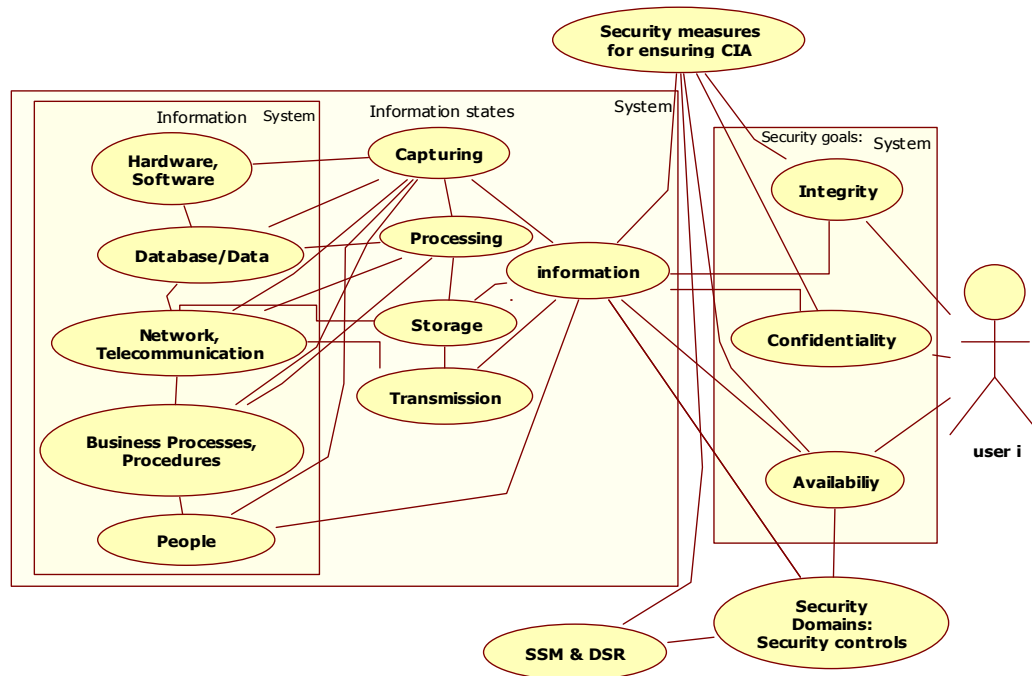


Figure 5.5: Information Systems Security Interrelations of Components

Key: CIA is an abbreviation for confidentiality, integrity and availability

Security requirements for enhancing the security of information systems have been presented in Figure 5.5. It has been defined in terms of components of IS (hardware, software, data, networks, business processes/procedures and people), information states, security measures, security controls for ensuring security goals (CIA triad), security domains, and soft design science (SSM integrated with DSR). The developed framework (Section 5.4.2) addresses the identified risks and incorporates

security requirements in terms of security measures and security controls for ensuring security goals (CIA triad) using multi-layered security approach for information in IS during information states in IS.

5.4.2 Developed framework for Enhancing Security of Information Systems

The framework for enhancing the security of IS provides a roadmap and guidance for effective assessment, identification and implementations of security measures and security controls for the protection of information resources (IT assets) against security breaches. It provides an explicit explanation of how the problem under study can be addressed by showing how the variables are related to each other. This framework has been developed to address the main research problem, the loss of security goals (CIA triad) for information in IS. It addresses the research question 3 (RQ3): "How to develop a framework for enhancing the security of information systems?" It provides guidance for the effective implementation of security mechanisms for ensuring security goals for information in IS.

The framework was developed based on addressing the identified research gap in the literature review (Chapter 2); using the findings of the results in Chapter 4, discussion of results in Chapter 5 and the established requirements in Section 5.4.1 for developing the framework for enhancing the security of information systems. These were all fused together by employing soft design science (SSM integrated with DSR) in a systematic circular iterative fashion until an optimal framework was obtained as presented in Figure 5.6. The developed framework for enhancing the security of information systems (Figure 5.6) mainly comprises of seven components; namely security requirement analyses, information security services (security goals),

information states, security measures, security controls, security domains and secured information system. The description of each of these components is as follows.

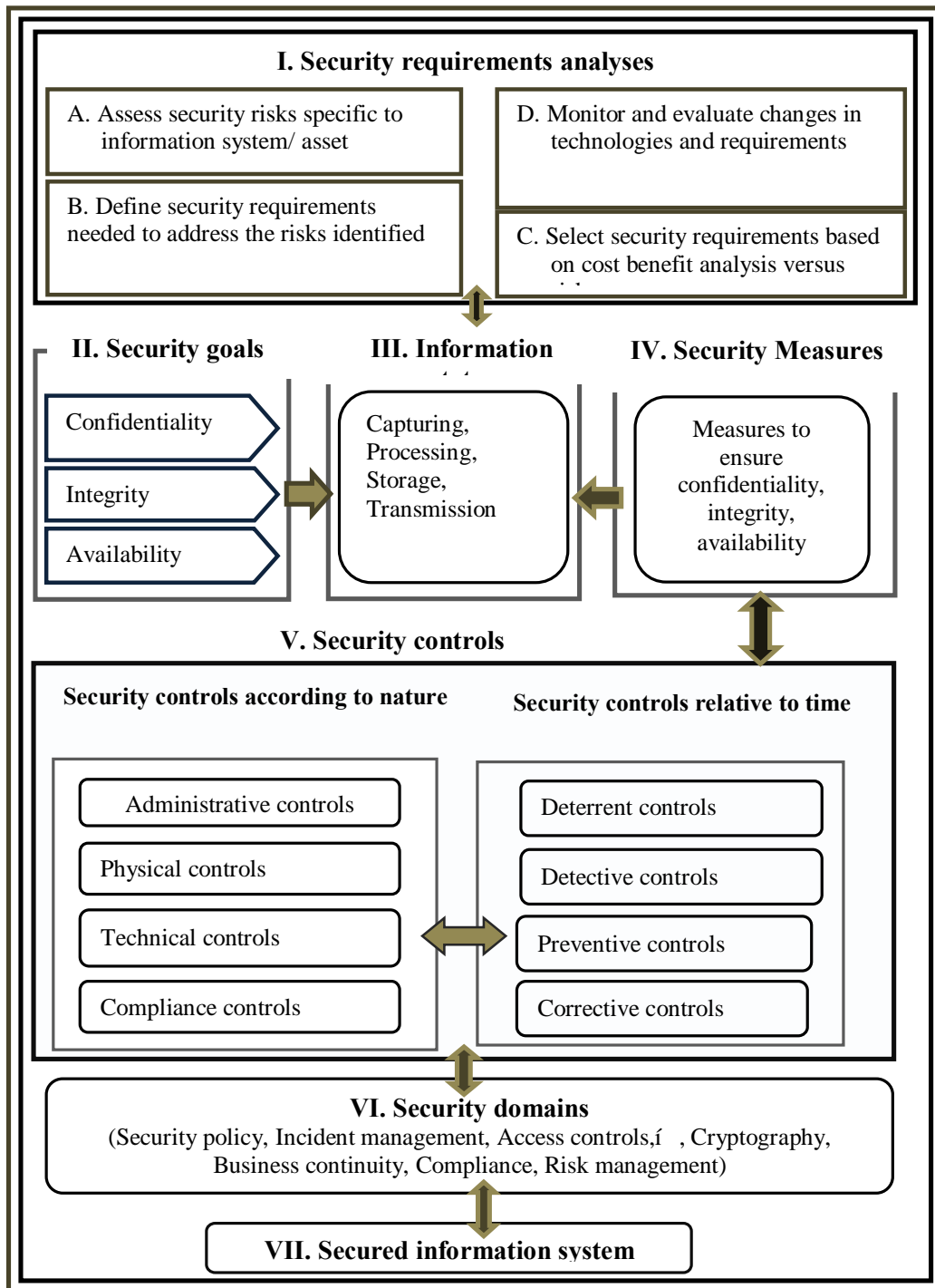


Figure 5.6: Framework for enhancing the security of information systems

The study proposes a framework for enhancing the security of information systems (Figure 5.6) which provide a roadmap and guidance for designing, creating/building a secure information system. It provides guidance by assisting in analysing security requirements. It first analyses the risks for the given information system to be developed and incorporates security requirements engineering principles during every stage of SDLC. It identifies security requirements in terms of security measures and security controls. It maps them to the appropriate security services (security goals) to ensure the security of information in IS during information states (capturing, processing, storage and transmission of information). The security controls are grouped and integrated into security domains and real world implementation layers.

The developed framework for enhancing the security of information systems in Figure 5.6 comprises of seven components, namely: security requirement analysis; information security services (security goals); information states; security measures; security controls and security domains and secured information system. The descriptions of each are as follows.

I. Security requirement analysis

- (a) Assess security risks specific to information system/asset
 - i. Assess risks and define security concerns specific the IS or application to be developed/acquired.
 - ii. Develop system architecture and classify all data involved in each transaction using approved data classification scheme: public, confidential, high confidential, secret, top secret.

- iii. Define security issues in terms of risks and their impact on the business process.
- iv. Prepare to be business process and develop its transactional flow diagram that tracks transactions various layers: presentation layer: client; network layer: Firewall, IPS/IDS; middle layer: Web-server(https), application layer: application server (IPsec, access control: OS, database); internal layer: Back end-servers (local database servers)
- v. Identify the criticality of application/information system to the business in the organisation

(b) Define security requirements to address the risks identified

- i. Create a possible list of security requirements (security measures and security controls) to address the identified risks
- ii. Mapp the security requirements with security services requirements

(c) Select security requirements based on cost benefit analysis versus risks

- i. Use cost based benefit to select for the best effective security measures and security controls based on a list in (b) above.
- ii. Consider implementation risks and the feasibility of implementing those security measures and security control by comparing the conceptual world and real world of concern

(d) Monitor and evaluate changes in technologies and requirements

Monitor for changes in technologies and changes in requirements due to business needs, changes in regulation, compliance requirements. Changes are

inevitable. The system security design architecture should be capable of accommodating changes in the future with minimal optimal efforts.

II. Information Security Services: Security Goals

The security services (known as security goals) can be categorized as availability, integrity, authenticity, confidentiality, privacy, and non-repudiation. The developed framework presents three categories of information security services (security goals), namely: confidentiality, integrity, and availability. The others are included in these three categories. For, example, integrity also covers authenticity and non-repudiation. Confidentiality includes privacy dimension.

(a) Confidentiality

Confidentiality is the prevention of intentional or unintentional unauthorized disclosure of contents information in IS. Maintaining confidentiality of the information in IS, requires that information in IS cannot be viewed or accessed by unauthorized persons or processes, and thus cannot be compromised. It implies keeping the information in IS private.

(b) Integrity

Integrity is concerned with the guarantee that the message sent is the one received and that the message is not intentionally or unintentionally altered. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle. The data integrity ensures that data has not been modified in transit. Integrity for data means that changes made to data are done only by authorized individuals, systems or processes. Corruption of data is a failure to maintain data integrity.

(c) Availability

Availability refers to the elements that create reliability and stability in IS. The availability is the timely, reliable access to information resources such as data, information; information services and IS for authorized users or processes. Availability is about information in IS being accessible as needed and where needed by authorized users, systems or processes. Availability ensures that IS and other IT resources are accessible when needed; allowing authorized users or processes to access them.

III. Information States

Within the information system, for any given moment, information is found in one or more of the four states: during capturing, processing, storage, and transmission. The security requirements for ensuring the security of information in IS should be defined in each information states. This is consistent with McCumber (1991), Maconachy & Ragsdale (2001) who created the NSTISSC security model (The McCumber Cube) for establishing and evaluating information security.

IV. Security Measures

Security measures are the course of actions taken to achieve a particular purpose; a procedure, initiative, operation to ensure security goals are guaranteed for information in IS. Some of the identified security measures for ensuring confidentiality, integrity, and availability (CIA) for information during information states (capturing; processing, storage, and transmission) in IS are summarized in Table 5.5.

Table 5.5: Security Measures for Ensuring Security Goals (CIA)

S/N	Security measures	Descriptions	Information states				Security goals		
			Capturing	Processing	Storage	Transmission	Confidentiality	Integrity	Availability
i.	Access control mechanisms	Implement selective restriction of access to a place or information resources such as audit logs and systems logs.	☒	☒	☒	☒	☒	☒	
ii.	Configuration management	Ensure correct configuration implementation for the information systems and ICT devices.	☒	☒	☒	☒	☒	☒	☒
iii.	Disabling/blocking insecure services, protocols/ports.	Disable or block insecure services, protocols, ports.	☒	☒	☒	☒	☒	☒	
iv.	Encryption of information/data	Encrypt sensitive information/data.	☒	☒	☒	☒	☒		
v.	Identification and authentication	Use a unique user account and password (something you know); security token such as smartcard (something you have); biometric (something your); digital certificates from trusted CA.	☒	☒	☒	☒	☒	☒	
vi.	Logging, monitoring of logs and alerting	Implement automatically logging, monitoring and alerting of security-related activities regularly.	☒	☒	☒	☒	☒	☒	☒
vii.	Media sanitization	Clearing, purging & destruction of data remanence prior disposal.	☒	☒	☒	☒	☒		
viii.	Network segmentation	Split network into subnets, VLANs; physical separation of LANs	☒	☒	☒	☒	☒	☒	
ix.	Patch management	Regularly patch the applications, operating systems, and ICT devices	☒	☒	☒	☒	☒	☒	☒
x.	Security awareness and training	Conduct security awareness and training for non-disclosure of sensitive information.	☒	☒	☒	☒	☒	☒	☒
xi.	Audit trail	Implement and monitor the audit trail (audit log) for a given sensitive information system.	☒	☒	☒	☒		☒	
xii.	Change management for IS	Implement change management and those changes should be documented, communicated, authorized, tested, implemented, monitored and audited to ensure the integrity of information.	☒	☒	☒	☒		☒	☒
xiii.	Checksum (or hash sum)	Implement checksum such as MD5/SHA3 to verify the integrity of data.	☒	☒	☒	☒		☒	
xiv.	Digital signature	Implement a digital signature to validate the authenticity and integrity of a message, software or digital document.	☒	☒	☒	☒		☒	
xv.	Integrity monitoring tools	Implement integrity monitoring tools for alerting of any unauthorized	☒	☒	☒	☒		☒	

S/N	Security measures	Descriptions	Information states				Security goals		
			Capturing	Processing	Storage	Transmission	Confidentiality	Integrity	Availability
		modification.							
xvi.	Least privilege principle/Need to know the principle	Implement procedures for reviewing users' access regularly, and only needed privileges should be applied and documented.	☒	☒	☒	☒		☒	
xvii.	Rotation of duties principle	Practice job rotation to breaks up opportunities for collusion and fraudulent activities.	☒	☒	☒	☒		☒	
xviii.	Segregation of duties principle	Duties should be sufficiently segregated in a given organization to ensure the detection of unintentional or unauthorized modification of information.	☒	☒	☒	☒		☒	
xix.	Backup strategies	Implement backup strategies based on the required point objective (RPO): loss acceptable; and required time objective (RTO): the time required to restore IS to operation after disaster or emergency.	☒	☒	☒	☒			☒
xx.	Business continuity plan(BCP)	Implement BCP; document and test regularly the BCP; no insurance that operations ever be restored to their present state in case of disaster.	☒	☒	☒	☒			☒
xxi.	Capacity planning	Predict and estimate the demand for IT assets.	☒	☒	☒	☒			☒
xxii.	Data backup process	The frequency of backup; labelling; retention period; the frequency of backup rotation.	☒	☒	☒	☒			☒
xxiii.	Disaster recovery plan	Document; specify procedures to be followed in case of an event of a disaster.	☒	☒	☒	☒			☒
xxiv.	Fault tolerance	Implement hardware and software redundancy; software recovery.	☒	☒	☒	☒			☒
xxv.	Incident management and response	Implement incident handling procedures; Functional incident response team and proper reporting.	☒	☒	☒	☒			☒
xxvi.	Monitoring of wired(LAN/WAN) and wireless networks	Continuously monitoring of LAN/WAN and wireless networks for unauthorized access.	☒	☒	☒	☒		☒	☒
xxvii.	Preventive maintenance	Regularly patching, updating antiviruses anti-malware, Operating systems.	☒	☒	☒	☒			☒
xxviii.	Protecting critical hardware and wiring from threats	Implement preventative measures to protect critical hardware and wiring from natural and man-made threats.	☒	☒	☒	☒			☒

S/N	Security measures	Descriptions	Information states				Security goals		
			Capturing	Processing	Storage	Transmission	Confidentiality	Integrity	Availability
xxix.	System monitoring mechanisms	Implement systems monitoring mechanisms.	☒	☒	☒	☒			☒
xxx.	Testing of the restore procedures	Test the restore procedures regularly.	☒	☒	☒	☒			☒

V. Security Controls

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, IS, or other assets. Security controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset. The security controls can be grouped according to nature or relative to time. These controls, when grouped according to nature, are classified as administrative controls, physical controls, technical controls, and compliance controls. These controls can further be grouped relative to time as deterrent controls, detective controls, preventive controls and corrective controls. Some of these security controls for ensuring security goals (CIA triad) are summarized in Table 5.4 in Section 5.3.

VI. Security Domains

The developed framework for enhancing the security of IS consists of 15 security domains. These security domains are namely: risk management; security policy; organisational of information security; human resources security; asset management, access controls; cryptography; physical and environmental security; operations security; communication security; systems acquisition, development, and

maintenance; supplier relationships; information security incidents management; business continuity; and compliance. Thus, for ensuring security goals (CIA) for information in IS during information states, effective security controls should be identified and implemented in each security domains (Table 5.4, Section 5.3).

VII. Secured Information System

The secured information system is the results of applying effective security requirements (security measures and security controls) for ensuring security goals (confidentiality, integrity and availability) during information states (capturing, processing, storage and transmission) in an information system. This involves doing requirements analysis to determine the security requirements for ensuring security goals (confidentiality, integrity and availability). This is followed by correct configurations, implementations, monitoring and evaluation as technologies changes/advances with time.

5.5 Human Sensor Web Prototype for Crowdsourcing Security Incidents

The section presents a discussion of the developed prototype for human sensor web for crowd sourcing information related to security incidents management. This prototype demonstrates the applicability of the developed framework for enhancing the security of IS in the real world environment. The prototype for human sensor web security incidents for managing information in the crowding was developed using human sensor web for a crowdsourcing information security incident. The choice of information security incidents management security domain was based on the fact that security breaches and subsequent incidents affecting IS in cyberspace are rapidly increasing at an exponential rate (Jang-Jaccard & Nepal, 2014; Nfuka et

al., 2014; Mshangi et al., 2015, 2016, 2017; Symantec, 2016, 2017). It was published in an international journal (Mshangi et al., 2018) as described in Appendix F, under paper V.

Managing incidents effectively involves detective and corrective controls designed to recognize and respond to events and incidents, minimize adverse impacts and gather forensic evidence (where applicable). Thus, in due course learn the lessons in terms of promoting improvements to the processes, typically by improving the preventive controls or other risk treatments (ISO/IEC, 2016). Thus, it involves preparing to deal with incidents; identifying and reporting information security incidents; assessing the incidents and making decisions. This includes patching things and getting back to business as quickly as possible or collecting forensic evidence; responding to incidents; learning the lessons, and making changes that improve the processes.

Consequently, information security incidents are bound to occur to some extent, even in organizations that take their information security extremely seriously. The study selected incident management security domain as a case study for developing a prototype for Human sensor web crowd sourcing information security incidents management. The research findings revealed that security incidents are on the rise. This is consistent with the previous studies by Jang-Jaccard & Nepal (2014), Nfuka et al. (2014) and Symantec (2017) who found that cybercrimes affecting IS in cyberspace are on the rise. The developed prototype serves as a tool for reporting, communicating, visualising the reported incidents in a geographical information system and responding to adverse events. This assists the incident response team

(IRT) in receiving, analysing, and responding to information security incidents affecting IS. This artifact (developed prototype) focuses on security incidents reporting and handling.

The developed artifact provides the following functionalities:

- i. The central part of this artifact is the database repository which stores information/data related to security incidents. This includes incident category, organisation affected, the impact on business processes, geographical information; solution/mitigation measures taken.
- ii. The artifact enables users to report and respond to various security incidents, using the web based - subsystem.
- iii. It provides functionalities for various stakeholders to request status/statistics of incidents reported; check for solutions about incidents happened previously in the sector and across the globe through SMS and the web-based functionalities.
- iv. It provides a platform for exchanging security incidents through geographical information system (GIS) and short message service (SMS). The information exchanged includes lessons learnt from viruses/malware attacks and hacking.
- v. It visualizes incidents happening using GIS in real time. Also, it visualizes incidents through histogram and charts

Thus, implementing effective security controls (such as reporting, responding in real time fashion) for managing security incidents improves the security of information in IS. The use of human sensor web (Mshangi et al., 2018), for handling security incidents facilitates in building reporting and responding security cultures to security

incidents in a timely fashion. This ensures the availability of information in IS. Also, reporting and responding to security incidents assists in mitigating risks related to violation of confidentiality and integrity of information in IS. It prohibits the spread of the impact of the security incidents across organizations and the education sector and the country in general.

5.6 Validation of the Developed Framework using Cryptographic

Techniques

This section presents the validation of the developed framework for enhancing the security of information systems using cryptographic techniques based algorithm for enhanced security. The framework comprises of seven layers (Section 5.4). One of these layers is security measures for ensuring confidentiality, integrity, and availability. Due to the limited resources and time; it is not feasible to simulate the whole framework. The study specifically demonstrates how to ensure the security of information in IS using cryptographic techniques based algorithm for enhanced security. This address research question 4: "How to validate the developed framework for enhancing the security of information systems?"

The study specifically employs cryptographic techniques to validate the proof of concept of the developed framework. It demonstrates how to ensure integrity, and confidentiality of information in IS. There are mainly three categories of cryptographic encryption techniques commonly in use. These are namely, asymmetric encryption (public key cryptography), symmetric key encryption (secret key cryptography) and hashing encryption. Asymmetric encryption uses different keys (private and public keys pairs) for encryption and decryption (Kessler, 2019);

for example RSA and Digital signature algorithm (DSA) schemes. It used for e-commerce and digital signature.

The other encryption scheme is the symmetric encryption where the same key is used for encryption and decryption; for example 3DES and AES (Bosworth et al., 2014; Kessler, 2019). It is fast for encryption and decryption, and it uses less computing resources as compared to asymmetric encryption but poses a challenge of key exchange. For practical use and a large volume of data, a hybrid of symmetric and asymmetric encryption can be adopted; by employing asymmetric encryption to address the problem of key exchanges in symmetric encryption.

Hashing function algorithm scheme is the one way encryption mathematical irreversible function used for computing fixed length hash value based on input message (Kessler, 2019). The hash value computed is unique irreversible value and it is used to provide a digital fingerprint (Bosworth et al., 2014; Kessler, 2019) to the content of the original message/file contents. It is used to verify the integrity of the message or file content (Bosworth et al., 2014). Examples hash algorithms include message digests (such as MD5 algorithm); and secure hashing algorithm (SHA) such SHA2 algorithm scheme (Kessler, 2019). The study adopts asymmetric encryption (also a combination with symmetric encryption can be employed) and hashing function algorithms schemes (such as SHA256) for validating the framework for enhancing the security of IS, case of education sector based on cryptographic techniques.

The study develops an algorithm for enhanced security based on cryptographic

techniques for validating the framework for enhancing the security of information systems. The study further develops a prototype using java object oriented programming. It validates proof of concepts of the developed framework for enhancing the security of information systems. The study demonstrates how to improve security by ensuring confidentiality and integrity of information in IS using the developed algorithm for enhancing security.

5.6.1 Security Requirements for Ensuring Security of Information and Information Systems using Cryptographic Techniques

The study employs cryptographic techniques to valid the developed framework for enhancing the security of information systems, a case study of the education sector in Tanzania. The security requirements identified are security requirements for ensuring confidentiality and integrity during storage and transmission of information in IS using cryptographic techniques. The study specifically employs hash, digital signature and encryption to ensure confidentiality and integrity of data during storage and transmission in IS.

Figure 5.7 represents security system architecture for validating the framework for enhancing the security of information systems based on cryptographic techniques. It portrays how to enhance security during storage and transmission in IS in untrusted environment settings such Internet based on cryptographic techniques. The security requirements for ensuring confidentiality and integrity for data stored and transmitted in an untrusted environment such as the Internet are presented. From Figure 5.7, the cryptographic security requirements for ensuring confidentiality and integrity during transmission in IS are presented as follows;

- i. Select a strong cryptographic algorithm scheme for ensuring confidentiality and integrity of information in IS during transmission in IS.
- ii. Generate the public key and private key for encrypting and decrypting information in IS. Let $private_{ks}$ and pub_{ks} represent the private key and public key respectively for encrypting and decrypting the input plaintext m_i .
- iii. The plaintext m_i is hashed using a hash function, $f_h(m_i, HashAlg)$ with effective hashing algorithm (HashAlg) such as SHA256. The output is a hash value (HashVlue). This ensures the integrity of the message, m_i
- iv. The hash value (digital finger print), $HashV alue$ is encrypted using the private key of the sender/data owner, $private_{ks}$ with function $Encr_k(hashValue, private_{ks})$ This encrypted hash value is called the digital signature of the plaintext message m_i
- v. The digital signature is attached or appended to the original plaintext message m_i to form a digitally signed message m_i' (plaintext + digital signature)
- vi. Encrypt the digitally signed message (plaintext + digital signature) with the public key, pub_{kr} of the receiver of the message using encryption function $Encr_K(m_i', pub_{kr})$, to form ciphertext c_i and send it the receiver
- vii. The receiver, decrypt the ciphertext c_i using the private key, $private_{kr}$ with function $Decrypt_k(c_i, private_{kr})$ to get the plaintext and signature of the message.
- viii. The receiver computes the hash value of plaintext message received using a hashing function, $f_h(m_i', HashAlg)$ with the same hashing algorithm $HashAlg$ as the

- sender, to get the hash value, $HashValue_{m_i}$
- ix. The receiver decrypts the digital signature, $sign$, using decryption function $decrypt(sign, public_{ks})$ to get the hash value, $HashValue_{sign}$
 - x. The receiver verifies the validity of the signature by comparing the two hash values, $HashValue_{m_i} = ? HashValue_{sign}$; if yes the signature is valid, it means integrity, authenticity, non-repudiation, authentication and accountability is maintained; else signature is invalid reject the message as probably was tempered, thus integrity, authenticity, non-repudiation, authentication and accountability cannot be guaranteed to the message m_i , communicate back

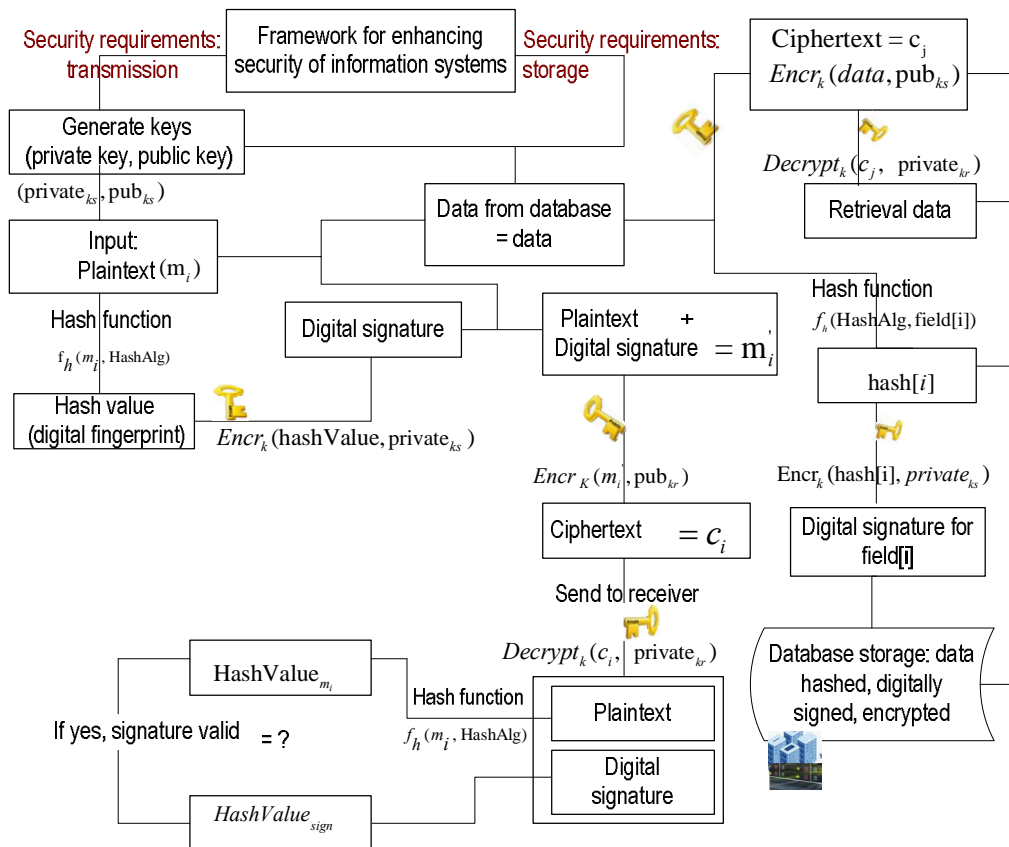


Figure 5.7: Security system architecture for validating the framework for enhancing the security of information systems using cryptographic techniques

Moreover, from Figure 5.7, security requirements for ensuring confidentiality and integrity based on cryptographic techniques during storage is presented as follows.

- i. Determine security requirements of data/information store in the database based on security clearance and data/information classification level
- ii. Encrypt data using the public key, pub_{ks} of the owner of data stored in the database at field level using encryption function $Encr_k(data, pub_{ks})$ to get ciphertext c_j . Store the encrypted ciphertext results into the given database tables. This ensures the confidentiality of data/information during storage in IS
- iii. Compute the hash value, $hash[i]$, using a hash function, $f_h(\text{HashAlg}, \text{field}[i])$ at field[i] based on the strong hashing algorithm, HashAlg, such as SHA256
- iv. Encrypt the hash value $hash[i]$ with a private key of the data owner using encryption function $Encr_k(hash[i], private_{ks})$; to get a digital signature, $sign[i]$ for field[i]
- v. Decrypt ciphertext c_j with a private key, $private_{ks}$ of the owner of data using decryption function $Decrypt_k(c_j, private_{ks})$ when needed.
- vi. Verify the integrity of data by re-computing hash, $hash[i]_{m_i}$ at the given field[i] and comparing with the hash [i] value, $hash[i]_{sign}$ obtained after decrypting the digital signature, $sign[i]$ at the corresponding field[i].
- vii. If the two hash values are equal, $hash[i]_{m_i} = hash[i]_{sign}$ then integrity, non-repudiations, authenticity, authentication and accountability is guaranteed during storage in IS. Else data were changed during storage and integrity, authenticity, non-repudiation, and accountability cannot be guaranteed.

5.6.2 Algorithm for Enhanced Security of Information Systems Using Cryptographic Techniques

To address the research question 4: "How to validate the developed framework for enhancing the security of information systems?" The study developed an algorithm for enhanced security using cryptographic techniques; specifically demonstrates how to ensure confidentiality and integrity of information in IS. To address the violation of confidentiality and integrity of information in IS; the study employs soft design science (SSM integrated with DSR) (Section 3.2). The conceptual models were compared with the actual world environment to the desirable changes for improvement.

The algorithm for enhanced security of IS was divide into sub-blocks. It was guided by soft design science in a systematic circular fashion (Section 3.2, Figure 3.2). It is based on security requirements (Section 5.6.1, Section 4.2 and Section 4.3). The developed algorithm for enhanced security of IS using cryptographic techniques is presented in Table 5.6. It validates proof of concept for the developed framework for enhancing the security of information systems, a case study of the education sector in Tanzania (Figure 5.7).

The developed algorithm for enhanced security is comprised of 7 blocks (Table 5.6), namely Algorithm block 1: Generate the key pairs; Algorithm block 2: Input plaintext message; Algorithm block 3: Creating hash value of message; Algorithm block 4: Creating digital signature and signing the original plaintext; Algorithm block 5: Encryption of digitally signed message; Algorithm block 6: Enhanced security during data storage; Algorithm block 7: Decryption of digitally signed

message, cipher c_i at receiving end.

Table 5.6: Algorithm for Enhanced Security Using Cryptographic Techniques

Algorithm block 1: Generate the key pairs

1. Generate the private and public key pairs ($private_k, pub_k$)
 $KeyPairGen = keyPairGenerator.getInstance(private_{ks}, pub_{ks});$
 2. Specify key length for the digital signature
 $KeyPairGen1.initialize(key_bitlength\ value);$
-

Algorithm block 2: Input plaintext message

1. Input plaintext: let msg be the plaintext message variable for storing m_i plaintext for student data during computational for message $i=1$ to n
 2. Plaintext, $msg = m_i$
-

Algorithm block 3: Creating a hash value of the message

1. Select the strong hash algorithm $HashAlg$ for computing hash value for message m
 2. Compute hash value, $hashValue$ using hash function H , $hashValue = H(msg, HashAlg)$
-

Algorithm block 4: Creating a digital signature and signing the original plaintext

1. Retrieval hash value, $hashValue$ and digitally sign it using a private key of the sender, $private_{ks}$
 2. Compute the digital signature $sign$ for hash value, $hashValue$ using encryption function, $Encr$ and with a private key of the sender $private_{ks}$
 $sign = Encr_k(hashValue, private_{ks})$
 3. Attach the digital signature to the original plain text message m
 Signed message m'_i using function f_{sig} ; expressed as $m'_i = f_{sig}(m_i, sign)$
-

Algorithm block 5: Encryption of digitally signed message

1. Retrieval the digitally signed message, m'_i
 $m'_i = f_{sig}(m_i, sign)$
 2. Encrypt digitally message m'_i using the public key of the receiver pub_{kr}
 Encrypted and digitally signed cipher text $c_i = Encr(m'_i, pub_{kr})$
 3. Send the Encrypted and digitally signed cipher text $c_i = Encr(m'_i, pub_{kr})$ to the receiver
-

Algorithm block 6: Decryption of digitally signed message, cipher c'_i at receiving end

1. Retrieval digitally signed cipher
 2. Decrypt digitally signed cipher c'_i ; $sign = m'_i = decrypt(c_i, private_{kr})$
 3. Verify the signature of the digitally signed message,
-

$hashValue_{sign} = decrypt(sign, public_{ks}) ;$

4. Compute, hash value using a hash algorithm $_{HashAlg}$ from the original message, m after decrypting digitally signed cipher c'_i ; $hashValue_{m_i} = f_h(m_i, HashAlg)$

5. Compare the two hash value in step 4 and 3 in this block 7

$if(hashValue_{sign} = hashValue_{m_i})$

then

6. Signature is verified as valid: authenticity, non-repudiation, integrity maintained

7. else

signature is invalid: authenticity, non-repudiation, integrity violation

Algorithm block 7: Enhanced security during data storage

4. Input plaintext: encrypt m using the public key of the data owner, pub_{ks}

5. UPDATE table[i]

6. For i=1 to n

{

7. $SET field[i] = ENCRYPTBYASYMKEY(field[i], pub_{ks})$

8. Hash field[i] using a hash function f_h using a strong hashing algorithm, $_{HashAlg}$;

$hash[i] = f_h(HashAlg, field[i]) ;$

9. Digitally sign the field i required

$DigitallySignField[i] = ENCRYPTBYASYMKEY(hash[i], private_{ks}) ;$

}

10. Decryption, input cipher retrieval $c_{[i]}$ from the database for n fields for decryption;

11. For i=1 to n

{

Select and assign to variable $field[i] = DECRYPTBYASYMKEY(c[i], private_{ks}) ;$

}

5.6.3 Illustration of Developed Algorithm for Enhanced Security

The algorithm for enhanced security of information in IS using cryptographic techniques was translated into a prototype computer application. The prototype was developed using java (Mikulcak et al., 2018) application program (Figure 5.8) with four classes as presented in Table 5.7. The source code for the prototype has been presented in Appendix D. The prototype consists of class reading input data (Reading Input Data); class for enhancing security of information during transmission state in IS (Enhanced Security Transmission Crypto Technique); class for enhancing security of information during storage in IS (Enhanced Storage

Security Crypto Techniques class); an main class calling other classes (Enhance Security of Information System) as summarized in Table 5.7.

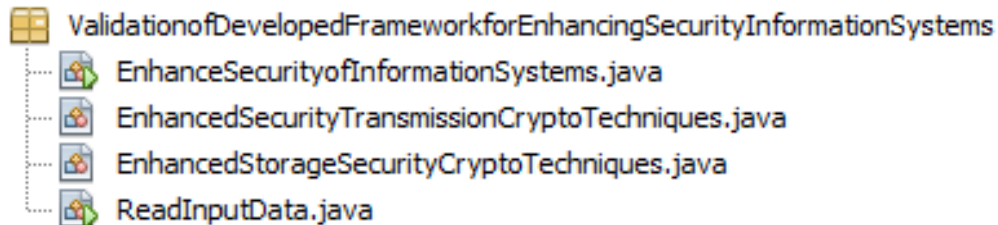


Figure 5.8: Snapshots of java classes for developed algorithm for enhanced security

Table 5.7 presents the summary of a description of each class in the developed algorithm for enhanced security of information systems using cryptographic techniques.

Table .5.7: Classes for a prototype for illustrating an algorithm for enhancing security

S/N	Class	Description
1	Enhanced Security Transmission Crypto Techniques	<ul style="list-style-type: none"> • This is class enhance the security of information in IS during transmission of information in IS in an untrusted environment such Internet. It ensures integrity and confidentiality using digital signature and hashing cryptographic techniques. It employs asymmetric encryption techniques to generates private and public key pairs; it creates hash values, and digital signatures based on the given hash values using a private key of the sender. • Moreover, it encrypts the digitally signed message with the public key of the recipient. This ensures authenticity, non-repudiation; integrity and confidentiality are maintained during transmission of information in IS between sender and receiver in an untrusted environment such as the Internet.
2	Enhanced Storage Security Crypto Techniques	<ul style="list-style-type: none"> • This is class enhance the security of information in IS during storage of information in IS in an untrusted environment such Internet. It encrypts data using the public key of data owner asymmetric encryption (private and public key pairs are used) at filed level; it uses a private key for decryption. • Moreover, it creates hash values for the given field and encrypts it using the private key (digital signature). Thus, it ensures confidentiality and integrity of information/data during storage in information systems
3	ReadingInputData	This class contains methods for reading and accepting input data plaintext to be secured in information systems.
4	Enhance Security of Information System	This is the main class which call other classes: Reading Input data; Enhanced Security Transmission Crypto Technique; and Enhanced Storage Security Crypto Techniques

5.6.4 Performance Analysis of The Developed Algorithm For Enhanced Security Based on Cryptographic Techniques Using a Controlled Experiment

The performance of the developed algorithm for enhanced security of information systems based on cryptographic techniques was analysed using a controlled simulation experiment. The simulation experiment was carried by out to validate how can the security of information be improved during information states in IS, a case study of the education sector in Tanzania. The experiment specifically shows performance analysis of the developed algorithm for enhanced security by ensuring the confidentiality and integrity of information during storage and transmission states in IS. The details, setup and execution of the simulation experiment follow.

5.6.4.1 Preparation of the Controlled Experiment

The following materials were prepared for conducting the controlled experiment

- i. Framework for enhancing the security of information systems security, a case study of the education sector in Tanzania
- ii. Algorithm for enhanced security for IS based on cryptographic techniques
- iii. Developed java prototype executable program of an algorithm for enhanced security of information systems based on cryptographic techniques
- iv. An input plaintext message is a file with 767 characters for simulating ensuring security during transmission in IS
- v. Input data from a database with student information sample extract (Student Phone; and Marks) of 9 records for simulating ensuring security during storage in IS
- vi. Laptop with Intel Core (TM) i5-4210U CPU @1.7 GHz 2.4 GHz processor, 8

GB RAM, 64-bit processor, Windows 10 64 bit Pro

- vii. Table template for recording results (Table A.3 in Appendix A)

5.6.4.2 The Objective of the Experiment

The objective is to perform validation of the developed framework for enhancing the security of information systems. To address this, the analysis of the performance developed an algorithm for enhancing the security of IS using cryptographic techniques. It employs asymmetric encryption and hashing techniques for demonstrating how to ensure confidentiality and integrity of information in IS.

5.6.4.3 Conditions for the Experiment

- i. Keys size was varied from 512 to 2048 bits
- ii. Input data was from a file and database
- iii. The experiment was simulated using end-user computing environment settings
- iv. The experiment was carried out in two phases and was carried for 10 iterations
- v. The average execution time was recorded in the table template for the experiment

5.6.4.4 Conducting the experiment

The Developed algorithm for enhancing security is based on cryptographic techniques. For validation of proof of concepts, the study adopted a Digital Signature Algorithm (DSA), RSA (Rivest, Shamir &Adleman) algorithm and secures hashing algorithms (SHA256). Other cryptographic public key infrastructure algorithms and hashing cryptographic techniques can be substituted to achieve the same results. The

byte code java program for the developed algorithm for enhancing security was executed by varying keys size from 512 to 2048 bits as shown in Figure 6.5. The simulation was performed in 10 iterations and average execution time computed was recorded in Table 5.8. The experiment is repeated for DSA and RSA by varying key size from 512 to 2048 bits to find out the optimal execution time and make a choose of a cryptographic algorithm for digital signature and encryption of plaintext message. Figure 5.8 depicts the execution time illustration for enhancing security during transmission state in IS using cryptographic techniques.

```

Output - ValidationDevelopedFrameworkEnhancingSecurity (run) X
Number of runs of simulation:
10
We are delighted to know that you have decided to join our university.
The Open University of Tanzania is the higher learning institution of your
Here you can pursue different higher education programmes through open, or
OUIDs Vision DTto be a leading open online University, in knowledge creati
the one of its own kind in Tanzania and East Africa,
in a unique position as an institution of higher learning that is
at the forefront of turning Tanzania into a middle income and
semi-industrialized country by daily churning out graduates who immediatel;
play a key role towards realization of the countryDs vision.
Message Digest: Hash value in Hex format :-ef14bacc707927408c771fc5d5d97a94
Digital signature for given text: 0=00000z(040s00#00000ND/00700D!00 r0AD D^
Signature verified is from the original source of message
Public Key used to decrypt/verify signature:Sun DSA Public Key
Parameters:
p:
8f7935d9 b9aae9bf abed887a cf4951b6 f32ec59e 3baf3718 e8eac496 1f3efd36
06e74351 a9c41833 39b809e7 c2aelc53 9ba7475b 85d011ad b8b47987 75498465

Simulation iteration:10

Enhance security: transmission simulation experiment
execution time for iteration:10=401ms

Sum of 10 iterations:transmission exceution time is :3104ms
For ensuring security during transmission in IS
Average execution time for: 10 iterations of the Alg.
enhanced security: transmission = 310ms
It employs cryptographic techniques to enhance security
  
```

Figure 5.9: Execution Results For Enhancing Security During Transmission in IS

From Figure 5.9 the input plain text message was read out from the data file as shown in Figure 5.9(a). The hash value was computed (Figure 5.9 (b)) and private and public pairs were generated. The computed hash value was encrypted with private of the sender (forming a digital signature, Figure 5.9(c)). This digital signature was attached to the original plaintext and a digitally signed message was encrypted with a public of the receiver (this ensure confidentiality of the information).

At receiving the encrypted cipher was decrypted using a private key of the sender (this ensure confidentiality); followed by verifying the digital signature (decrypting digital hash value cipher using the public key of the sender) and computing the hash value from the original plaintext message. The key size was varied from 512 to 2048 and the execution time was recorded in Table 5.8. The execution time for 10 iterations for a key size of 2048 was 310 milliseconds (ms) as shown in Figure 5.9(f). This ensures confidentiality, authenticity, non-repudiation and integrity of plain message in general during transmission in information systems.

Figure 5.10 depicts the execution of enhancing the security of IS during storage state in IS. For addressing how security can be improved during storage in IS, the study employed controlled simulation experiment accepted input data from the database for student information detail. The fields with sensitive confidential information such as student phone numbers, marks for the given subject are secured using cryptographic techniques (Figure 5.10 and Table 5.8). The study employed the RSA algorithm for encrypting data at the field level as summarized in Table 5.8. The data in field such marks are encrypted using the public key of the owner/custodian of data

and can be decrypted by the corresponding private key. This ensures the confidentiality of data/information during storage in IS.

```

10000 E71B047A33381800073F774BE3B8F3C88C7B2B3B1712335026336BB291750B171FB237BAC28F7E65A3E8I
10001 01C4C7607ABB83B6B89F33BA80C48DB5D6B103E1564152B5DA875DD08555D8397D04D192EBAE01B2D712:
10002 D8EA3566FA5391CF00F52F72AAA9BF9BAA9DD080DAAE7F9737E0C3DAF3D4EEF9DD51E6F204F8348F6DB3:
10004 29F3DC29A5F7A556B7A2C0CE41F3148D5EE9707DF92C42DF8B015BA5D6995328BADCF1FE8F2AB4AD04C6'
10005 E670457C8A114CBB9A28590459E6738B3E701F0E543FA67D866544336BB04F3F98078C6013E5BCE2A6834
10006 67DD1007D2A99E9C00689098FEA6C7CD98DEC490D74BF20674A48D3D2212B48F7262CE1335EC079EDC86I
10007 83EBE4D321B870485B7F36A06559618B1CCE2BCEE257A763681E12EE1B66B5B034F55E8727D5554CAC80I
10008 EFE673B786A3A975CB42EBA3D8D9CA3FFE3B84A5377FEF92C0CE194F9FF70A14302248620F5FAFBFD81AI
10009 0601B466E5173BEECB1221A35C8C3B51033137F43EABDD744A2E7AAB0A3C49A1E1C32D3FE6B3FF746714
Simulation iteration:10

Enhance security: storage simulation experiment execution time for iteration:10=1099ms

Sum of 10 iterations execution time is :9684ms
For ensuring security during storage in IS
Average execution time for: 10 iterations of the Alg. enhanced security: storage, = 968ms
It employs cryptographic techniques to enhance security

```

Figure 5.10: Encrypted Results in Table Fields During Storage in IS

Furthermore, for ensuring integrity during storage, hash values were computed at fields level using hash cryptographic algorithm SHA256. The computed hash values were encrypted using a private key of the data owner (creating digital at field level in a database) as shown in the column 'Digitally Signed Marks' in Table 5.8. This ensures integrity and authenticity, non-repudiation, and accountability of data stored in the database such as students marks and phone numbers.

Table 5.8: Enhancing Security During Storage in IS Using Crypto Techniques

StudentId	SubjectCode	HashedStudentPhone	EncryptedMarks	HashedMarks	DigitallySignedMarks
10000	200	0x01D653C7F0102...	0xAD27CF069...	0x2A38A4A...	0x953857466E50...
10001	200	0x3CD6CFC77DDE...	0x6EE65C381...	0xAC627AB...	0x67E277B9883...
10002	200	0x964F0E460372A...	0x40D08DB3...	0xD09BF41...	0x1292694EB86...
10004	200	0xA72C931DABEC...	0xD8D9C5F8...	0x34173CB...	0x78CF1A99F7B...
10005	200	0x845840F81B386...	0x37795E43E...	0xD3D9446...	0xA8D0864A580...
10006	200	0x45E9720BA210D...	0x7B8F91E03...	0x8613985E...	0x3790926E761C...
10007	200	0x61BA27C87BBA...	0xE024CFAC2...	0xE2C420D...	0x085D5450B1C...
10008	200	0x0A3A69C14F440...	0x526C02EA2...	0xAD61AB1...	0x411D09ECFB4...
10009	200	0x17616B4D7E933...	0x69F19994B...	0xD2DDEA...	0x7B23572EE91...

5.6.4.5 Results of the Controlled Experiment

The experiment involved varying cryptographic algorithms and varying key sizes from 512 to 2048. The average execution time in milliseconds for every 10 iterations for enhancing security during transmission and storage in IS was recorded in table template as shown in Table 5.9.

Table 5.9: Results of Execution Time For A Simulation Experiment

Key size (bits)	Execution Time(ms): Transmission		Execution Time(ms): Storage
	DSA& SHA256	RSA& SHA 256	RSA
512	319	604	1339
1024	436	1058	1464
2048	535	3456	1623

The data results were analysed using Microsoft Excel and were visualized using the histogram as shown in Figure 5.11 and Figure 5.12. Figure 5.11 presents the execution time of an algorithm for enhanced security of IS based on cryptographic techniques. in the size of keys employed and the given cryptographic techniques adopted.

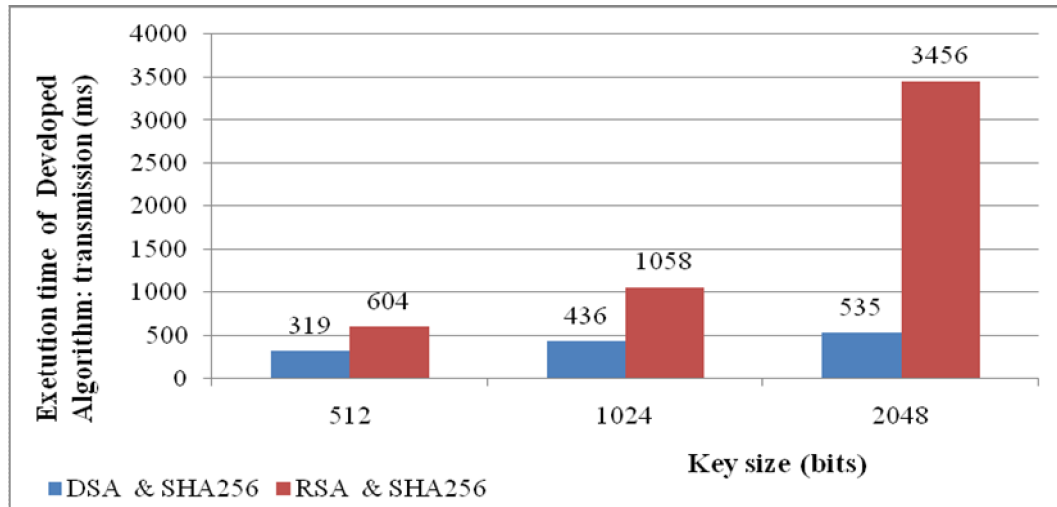


Figure 5.11: Results execution time for enhancing security during transmission in IS

Figure 5.11 presents the execution time from keys generation, reading the input plaintext message, computing hash value, digitally signing, encrypting, sending a secured message to the receiving end in untrusted environment settings such Internet. Also includes time for decrypting and verifying the digital signature at the receiving end. The results in Figure 5.11 shows that DSA has less execution time compared with RSA during digitally signing and varying the digital signature. This shows that the execution time of the algorithm for enhancing the security of information in IS based on cryptographic techniques increases with increase.

Analysis of data collected for encryption, digital signing and decryption of encrypted during storage is depicted in Figure 5.12. The results study of simulation controlled experiment in Figure 5.12 shows that execution time increases with the increase in key sizes for cryptographic based techniques such as asymmetric encryption by RSA cryptographic algorithm.

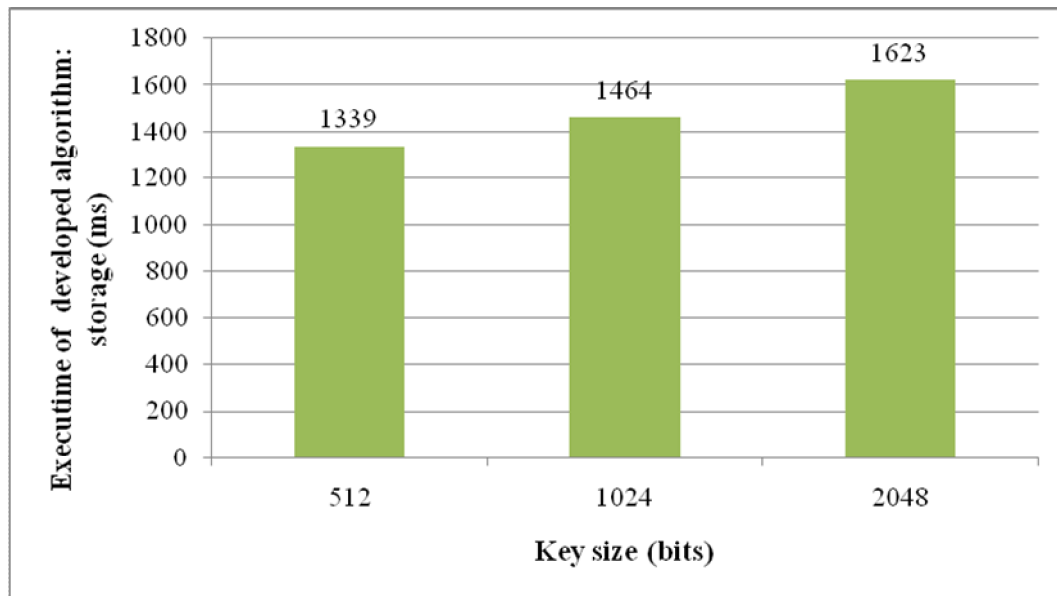


Figure 5.12: Results Execution Time for Enhancing Security during Storage in IS

The study recommends for digital signing of the normal plaintext message, DSA should be used. For encryption and decryption of data RSA cryptographic algorithm should be adopted.

5.6.5 Discussion of the Validation of the Developed Framework for Enhancing the Security of Information

Based on results validation results presented from Section 5.6.1 to 5.6.4, the study found that the developed framework for enhancing the security of information systems can be adopted to improve the security of information in IS. Based on the developed algorithm in Section 5.6.2 and its validation in 5.6.4 through simulation controlled experiment the study was able to validate (Mikulcak et al., 2018) how to enhancing security in information systems by ensuring confidentiality and integrity during transmission and storage in IS.

The study in the controlled simulation experiment revealed that the execution time for digitally signing, verifying digital signature and encryption during transmission and storage using cryptographic techniques based on DSA with SHA 256 is less than 535 ms for a key size of 2048 for 767 characters. Additionally, it was found that the execution time was less than 436 ms for a key size of 1024 bits length; and it was less than 319 for a key size of 512 bit length. The study recommends using DSA with a key size of 1024 and SHA 256 for digitally signing; as the execution time is still less (tested for a message with 767 characters). For a real world production environment, the study recommends RSA with a key size of 1024 bit length (execution time less than 1.058 seconds for 9 records for encryption and decryptions). Its security level is high; the higher the key size the stronger the security. The study found that the performance result of the proposed solution is consistency with other studies in the literature (Othman et al., 2007; Aufa et al., 2018; Mseteka et al., 2019). A study by Aufa et al. (2018) found an execution time of 14,455 ms for combined RSA 1024 and DSA 512 key size.

5.7 Evaluation of the Framework for Enhancing the Security of Information Systems

This section presents the evaluation of the developed framework for enhancing the security of information systems. It presents Method Evaluation Model which was adopted to assist the evaluation of the developed framework. Moreover, it presents how the evaluation exercise was conducted, and the results of the evaluation of the developed framework for enhancing the security of information systems. This addresses research question 5: "How to evaluate the developed framework for

enhancing the security of information systems?ö

The study employed the Method Evaluation Model (MEM) (Moody, 2003) for evaluating the developed framework for enhancing the security of information systems. MEM is the method for evaluating IS design artefacts such as methods, models and frameworks (Moody, 2003; Elias, 2015). The MEM was adopted because it incorporates both aspects of evaluation in term of performance and user perception.

The MEM was first employed to evaluate the performance in terms of efficiency, effectiveness and efficacy using a simulation controlled experiment. Secondly, it was employed to measure the perception of users (perceived ease of use and perceived usefulness) of the developed framework for enhancing the security of IS (Moody, 2003; Elias, 2015).

5.1.1 Performance of the Developed Framework For Enhancing Information Systems Security

The study evaluated the performance in terms of efficiency, effectiveness and efficacy using a simulation controlled experiment as presented in section 5.6.4.

5.1.1.1 The Efficiency of the Developed Framework For Enhancing the Security of Information Systems

Efficient of the developed framework for enhancing the security of information systems refers to the framework using minimum effort or resources while

implementing security controls and security measures for ensuring the security of information in IS. The study revealed that the execution time is 319 ms for DSA cryptograph algorithm for a key size of 512 bits when the controlled experiment was carried out for 10 iterations.

The execution time increases with the increase in key size; for example for a key size of 2048, the execution time was 535 for the DSA algorithm and was 3,450 ms for the RSA encryption algorithm. By evaluating the execution time, the key size of 512 bit has the minimum execution time of 319 ms as shown in Table 5.10; it uses less computing resources as compared to other keys. It can be employed for encryption and decryption of plaintext message. But the higher the key size the harder to break the key; the key size of 1024 bit can be adopted.

5.1.1.2 Effectiveness of the Developed Framework For Enhancing The Security Of Information Systems

Effectives of the developed framework refers to its adequate in accomplishing the objective of improving the security of IS and producing the intended or expected results. The study employed a controlled simulation experiment to evaluate the effectiveness of the developed framework for enhancing the security of IS as presented in section 5.6.4. The data were hashed, digitally signed and encrypted. This shows that confidentiality is achieved through encryption. Integrity, authenticity, non-repudiation and authenticity of data/information in IS is achieved as presented in Figure 5.8 and Figure 5.9. The framework for enhancing the security of IS is effective. It achieves the intended security objectives.

5.1.1.3 Efficacy of the Developed Framework For Enhancing The Security Of Information Systems

The efficacy of the developed framework refers to the ability or capacity of the framework to improve the security of information in IS. The study employed a controlled simulation experiment (Section 5.6.4) to evaluate the efficacy of the developed framework for enhancing security, case of the education sector in Tanzania. The capacity and power of ensuring the security of IS depend on the strengths of the keys. The higher key size the greater the strength of the algorithm. Based on execution time in Table 5.9; the key size of 2048 has the highest execution time of 535 ms for RSA and 3,450 ms for RSA. It is considered more efficacies to hackers or cryptanalysis. Thus, it is recommended to use a strong key size such as DSA and RSA with SHA256.

5.1.2 Perception of Users for the Developed Framework

5.1.2.1 Perceived Ease of Use

Researchers (Davis, 1986; Moody, 2003; Elias, 2015) has argued that the perceived ease of use is the key role in the evaluation of the developed framework such as the framework for enhancing the security of IS. According to Davis (1986), perceived ease of use is the degree to which a person believes that using the framework for enhancing the security of IS would be free from effort. The evaluation was carried out through experiment for evaluation of the developed framework for enhancing the security of IS. The users exercised using the framework for enhancing the security of IS through an experiment using an electronic assessment tool (Educause.edu, 2015). This was followed by completing an online post-survey questionnaire. The survey

questionnaire questions for evaluating the perceived ease of use are summarized in Table 5.10. The online post-survey questionnaire was based on a Likert scale with 5 points: strongly disagree, disagree, neither, agree, and strongly agree.

Table 5.10: Evaluating the performance: perceived ease of use

Items	Statement	Likert Scale
E1	I find a framework for enhancing the security of information systems is easy to use (E1).	<input type="radio"/> Strongly disagree <input type="radio"/> Disagree <input type="radio"/> Neither <input type="radio"/> Agree <input type="radio"/> Strongly agree
E2	It is easy for me to learn how to use the framework for enhancing the security of information systems (E2).	<input type="radio"/> Strongly disagree <input type="radio"/> Disagree <input type="radio"/> Neither <input type="radio"/> Agree <input type="radio"/> Strongly agree
E3	It is easy to become skilful at using the framework for enhancing the security of information systems (E3).	<input type="radio"/> Strongly disagree <input type="radio"/> Disagree <input type="radio"/> Neither <input type="radio"/> Agree <input type="radio"/> Strongly agree

5.1.2.2 Perceived Usefulness

Researchers Davis (1986); Maranguni & Grani (2015) argued that perceived usefulness is another key role in the evaluation of the developed framework. According to a study by Davis (1986), perceived usefulness is the degree to which a person believes that using a framework for enhancing the security of IS would enhance the security of information during information states (capturing, processing, storage and transmission) in IS. The evaluation of the developed framework for enhancing the security of IS was carried out to determine the perceived usefulness. This was done by carrying out an experiment to determine perceived usefulness for the developed framework for enhancing the security of IS using an electronic assessment tool (Educause.edu, 2015). This was followed by filling out a survey questionnaire. The survey questionnaire research question for evaluating the

perceived ease of use is summarized in Table 5.11. The survey questionnaire was based on a Likert scale with 5 points: strongly disagree, disagree, neutral, agree, and strongly agree.

Table 5.11: Evaluating the perceived usefulness

Item	Statement	Likert scale
U1	The developed framework for enhancing the security of information systems would improve the security of information in information systems (U1).	<input type="radio"/> Strongly disagree <input type="radio"/> Disagree <input type="radio"/> Neither <input type="radio"/> Agree <input type="radio"/> Strongly agree

5.1.3 Experiment Evaluating Perception of Users of the Framework

The experiment was carried out to determine the perceived ease of use and perceived usefulness of the developed framework for enhancing the security of IS. The experiment involved the preparation of the experiment in terms of materials and participants. The experiment was executed in two phases and the results were recorded in table format after execution. The details are presented as follows.

5.1.3.1 Preparation of the Experiment

The following materials were prepared and given to participants of the experiment for evaluating the developed framework for enhancing the security of IS

- i. A copy of the developed framework for enhancing the security of information systems (Mshangi et al., 2017) with descriptions of its components
- ii. Extract of the electronic assessment tool (Educause.edu, 2015) for practising on how to improve the security of IS using the developed framework for enhancing the security of IS.
- iii. An onlinepost-survey questionnaire based on TAM for evaluating perceived

ease of use and perceived usefulness of the developed framework for enhancing the security of IS.

5.1.3.2 Conducting the Experiment

Forty participants (IT experts from seven organizations under study) were invited to participate in the experiment for evaluation of a framework for enhancing the security of IS. The participants were given the required materials for conducting the experiment. The experiment was conducted using an electronic assessment tool (Educause.edu, 2015). This was followed by completing an online survey questionnaire after doing the experiment. The respondents were given 10 days to do the experiment and respond to the online survey questionnaire. The response was 31 participants out of 40 participated in the experiment; this gives a response rate of 77.5 %.

5.1.4 Experiment Results for Evaluation of a Framework for Enhancing Security of Information Systems

This section presents the results of the evaluation of the developed framework for enhancing the security of information systems. The evaluation criteria were based on perceived ease of use and perceived usefulness of the developed framework for enhancing the security of information systems. The results and discussions are presented as follows.

5.1.4.1 Perceived Ease of Use

Chi-square goodness of fit test with 0.05 significance level and $df = 4$ was carried out to determine the significance level of perceived ease of use for the developed

framework for enhancing the security of IS. The following hypotheses were formulated and tested for significant contribution using Chi-square goodness of fit test at a 95% confidence interval ($\alpha=0.05$).

Hypothesis 1

The elements definition of the framework for enhancing the security of IS are clear and helpful for improving the security of IS.

The study used descriptive statistics and non-parametric statistics test using Chi-square goodness of fit test at 95% confidence interval ($\alpha=0.050$) to test the significance perceived ease of use (elements definitions are clear and helpful) of the developed framework for enhancing the security of IS. The finding results are as follows.

Table 5.12 depicts the views when respondents were asked whether the definition of the element of the framework for enhancing the security of IS are clear and helpful for improving ISS. The findings depicted that, the majority of respondents (more than 96.8%) revealed that elements definition of the framework for enhancing the security of IS are clear and helpful for improving ISS with a median of 2. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 31) = 57.54, p < .05$) in Table 5.12 revealed that the definition of the element of the framework for enhancing the security of IS are clear and helpful for improving ISS.

Table 5.12: Elements of the developed framework are clear and helpful

S/N	Category	Observed N	Expected N	Residual	Percent
1	Strongly agree	8	6.2	1.8	25.8
2	Agree	22	6.2	15.8	71.0
3	Neither	1	6.2	-5.2	3.2
4	Disagree	0	6.2	-6.2	0
5	Strongly disagree	0	6.2	-6.2	0
Total		31			100
$\chi^2(5, N = 31) = 57.54, df=4, p = .000; \text{median} = 2$					

Hypothesis 2

It is easy to learn how to use the framework for enhancing the security of IS.

The study used descriptive statistics and non-parametric statistics test using Chi-square goodness of fit test at 95% confidence interval ($\alpha = 0.050$) to test the significance perceived ease of use (easy to learn on how to use the framework) of the developed framework for enhancing the security of IS in improving the security of IS. The finding results are as follows.

Table 5.13 depicts the views when respondents were asked whether it is easy to learn on how to use the framework for enhancing the security of IS. The findings depict that the majority of respondents (more than 93.5%) revealed that it is easy to learn on how to use the framework for enhancing the security of IS with a median of 2. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 31) = 73.032, p < .05$) in Table 5.13 revealed that it is easy to learn on how to use the framework for enhancing the security of IS.

Table 5.13: Framework for Enhancing the Security of IS is Easy to Use

S/N	Category	Observed N	Expected N	Residual	Percent
1	Strongly agree	4	6.2	-2.2	12.9
2	Agree	25	6.2	18.8	80.6
3	Neither	2	6.2	-4.2	6.5
4	Disagree	0	6.2	-6.2	
5	Strongly disagree	0	6.2	-6.2	
Total		31			
$\chi^2(5, N = 31) = 73.032, df=4, p = .000; \text{median} = 2$					

Hypothesis 3

It is easy to become skilful on using the framework for enhancing the security of information systems.

The study used descriptive statistics and non-parametric statistics test using Chi-square goodness of fit test at 95% confidence interval ($\alpha = 0.050$) to test the significance perceived ease of use (easy to become skilful at using the framework) of the developed framework for enhancing the security of IS in improving the security of IS. The finding results are as follows.

Table 5.14 depicts the views when respondents were asked whether it is easy to become skilful on using the framework for enhancing the security of IS (E3). The findings depict that the majority of respondents (more than 93.6%) revealed that it is easy to become skilful at using the framework for enhancing the security of IS (E3) with a median of 2. Moreover, the Chi-square goodness of fit test results

($\chi^2(5, N = 31) = 80.129$, $p < .05$) in Table 5.14 revealed that it is easy to become skilful at using the framework for enhancing the security of IS.

Table 5.14: Skillful at Using The Developed Framework

S/N	Category	Observed N	Expected N	Residual	Percentage
1	Strongly agree	3	6.2	-3.2	9.7
2	Agree	26	6.2	19.8	83.9
3	Neither	2	6.2	-4.2	6.5
4	Disagree	0	6.2	-6.2	0
5	Strongly disagree	0	6.2	-6.2	0
Total		31			0
$\chi^2(5, N = 31) = 80.129$, $df = 4$, $p = .000$; median = 2					

5.1.4.2 Perceived usefulness

Chi-square goodness of fit test with 0.05 significance level and $df = 4$ was carried out to determine the significance level of perceived usefulness for the developed framework for enhancing the security of IS. The following hypothesis was formulated.

Hypothesis

The developed framework for enhancing the security of IS will improve the security of IS.

The study used descriptive statistics and non-parametric statistics test using Chi-square goodness of fit test at 95% confidence interval ($\alpha = 0.050$) to test the significance usefulness of the developed framework for enhancing the security of IS in improving the security of IS. The finding results are as follows.

Table 5.15 depicts the views when respondents were asked about the developed framework for enhancing the security of IS would improve the security of IS. The findings depict that the majority of respondents (100%) revealed that the developed framework for enhancing the security of IS would improve the security of IS with a median of 2. Moreover, the Chi-square goodness of fit test results ($\chi^2(5, N = 31) = 60.129, p < .05$) in Table 5.15 revealed that the developed framework for enhancing the security of IS would improve the security of IS.

Table 5.15: Developed framework would improve the security of information systems

S/N	Category	Observed N	Expected N	Residual	Percentage
1	Strongly agree	9	6.2	2.8	29
2	Agree	22	6.2	15.8	71
3	Neither	0	6.2	-6.2	0
4	Disagree	0	6.2	-6.2	0
5	Strongly disagree	0	6.2	-6.2	0
Total		31			100
$\chi^2(5, N = 31) = 60.129, df = 4, p = .000; \text{median} = 2$					

5.8 Discussion of the Evaluation of the Developed Framework for Enhancing Information Systems Security

The study employed cryptographic algorithm based techniques for validation of the developed framework for enhancing the security of information systems (Section 5.6). It simulated how to ensure confidentiality and integrity of information during storage and transmission in IS using cryptographic techniques. The capacity and power of ensuring the security of IS using cryptographic techniques depend on the strengths of the keys. The higher key size the greater the strength of the algorithm. The study employed a key size from 512 to 2048 for encryption and decryption

using RSA. It employed DSA for digital signing of plaintext data to ensure its integrity, authenticity and non-repudiation. It recommends adoption of the proposed solution in a real world environment with the key size of 1024 bits for ensuring confidentiality and integrity of information during capturing, processing, storage and transmission in IS.

The problem of loss of CIA triad of information in IS can be addressed using the developed multi-layered security framework for enhancing the security of IS. It involves implementing security measures and security controls in different layers of security in accordance with security requirements. Thus, security can be enhanced during capturing, processing, storage, and transmission in IS by ensuring security goals (confidentiality, integrity and availability) using the developed framework for enhancing the security of IS. The evaluation results (Section 5.7) revealed that the developed framework for enhancing the security of information systems was widely accepted by target organizations in the education sector in Tanzania (Section 5.7).

The developed framework (Section 5.4.2) for enhancing the security of information systems can be used in real world environment settings to improve the security of information in IS (Mshangi et al., 2017). The evaluation results are consistent with other results studies in the literature (Bakari, 2007; Lupiana, 2008; Chatfield, 2009; Karokola et al., 2013; Mbowe et al., 2016; Razali, 2018; Mseteka et al., 2019; Nyamtiga et al., 2019). The proposed solution for enhancing the security of information systems have been employed by Mseteka et al. (2019) for securing examinations results of students during storage and transmission of Zambia's

Technical Education Vocational and Entrepreneurship Training Authority (TEVETA). Additionally (Razali, 2018) applied the proposed solution (Mshangi et al., 2017) while developing a Community Based E-Museum Framework for Sustainable Cultural Heritage Information System.

The developed framework for enhancing security of IS has been started to be used by some organizations in education sector in Tanzania; this is evidenced by Organisation M. It applied the proposed solution to address the problem of loss of availability of information in IS during release of National examinations results in Tanzania; such as form two, form four and form six exams results (February 2019 to January 2020). The organisation M used a content delivery network (CDN) technology to address the loss of availability of information in IS during the dissemination of exams results. CDN is a distributed system of servers which delivers web contents to users using caching, based on users' geographic locations requests (Cloudflare, 2019) through load balancing of heavy traffics for fast delivery with enhanced security.

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

6.1.1 Research Summary

The study assessed and identified security requirements (security measures and security controls) for ensuring security goals (confidentiality, integrity and availability) for information in information systems. The research process was managed by the soft systems methodology integrated with design science research (termed as soft design science). In addition, the soft design science methodology was compounded with mixed research methodology (i.e. qualitative and quantitative research methodology were used). This holistic approach helped in research methodology triangulation.

The study carried out a maturity level assessment for security status quo to determine security requirements gap (security measures and security controls). For assessing the security status quo, the study applied SSE-CMM with a rating scale of 0 - 5 to determine the maturity level. In the SSE-CMM rating scale of 0-5; 0 being the minimum and 5 is the maximum maturity level. The study found that maturity level across security domain is 1 and institutional security maturity level is 1 in SSE-CMM rating scale 0-5 in the education sector in Tanzania.

The finding shows that the implementation of security measures and security controls for ensuring security goals (CIA) are implemented in ad-hoc. Thus, for improving the security of information during information states (capturing, processing, storage, and transmission) in information systems, organisations should

implement effective security measures and security controls for ensuring security goals in each security domain (multilayer security).

The study developed a prototype for human sensor web crowd sourcing information related to security incidents management. The prototype demonstrated the applicability of the developed framework for enhancing the security of IS in real-world environment settings. Furthermore, the developed framework was validity using a cryptographic based algorithm. The study developed a cryptographic based algorithm to validity the proof of concept for the developed algorithm. It revealed that the execution time for the developed cryptographic algorithm for ensuring integrity and confidentiality using DSA with SHA 256 is less than 535 ms for a key size of 2048 for 767 characters. Additionally, it was found that the execution time was less than 436 ms for a key size of 1024 bits length; and it was less than 319 for a key size of 512 bit length for RSA. The higher key size the greater the strength of the algorithm. Moreover, the developed framework for enhancing the security was evaluated using a controlled experiment which was guided by the Method Evaluation Model. The study evaluated the developed framework for enhancing the security of IS for its performance, perceived ease of use and perceived usefulness in improving the security of IS.

The problem of loss of confidentiality, integrity and availability of information in IS can be addressed using the developed multi-layered security framework for enhancing the security of IS. It involves implementing security measures and security controls in different layers of security in accordance with security requirements. Thus, security can be enhanced during capturing, processing, storage,

and transmission in IS by ensuring security goals (confidentiality, integrity and availability) using the developed framework.

6.1.2 Answers to Research Questions

The main research problem was the loss of confidentiality, integrity and availability of information in information systems. Three research questions were formulated to guide the research process. These research questions aimed at addressing the main research objective. The main research objective was to assess security requirements (security measures and security controls) and develop a framework for enhancing the security of information systems in Tanzania: the case of the education sector. This section presents a summary of the answers to research questions based on the research study findings.

Research Question 1: To what extents are the existing security measures ensure confidentiality, integrity and availability of information in information systems?

Response: Based on the literature review in Chapter 2, Research Methodology in Chapter 3, Research Findings in Chapter 4 and Discussion of the Results in Chapter 5; the study assessed and identified security measures for ensuring confidentiality, integrity and availability of information during information states (capturing, processing, storage and transmission) in information systems. The security measures for ensuring confidentiality, integrity and availability of information in information systems during information states (capturing, processing, storage and transmission) has been assessed and identified as summarized in Section 5.2 (Table 5.1, Table 5.2, Table 5.3).

The study proposes authentication authorization system architecture for ensuring confidentiality of information and information systems (Figure 5.1). It proposes crypto system architecture for ensuring confidentiality of information and information systems as presented in Figure 5.2 in Section 5.2.1. Moreover, it proposes cryptographic systems architecture for enhancing the integrity of information and information systems as presented in Figure 5.3 in Section 5.2.2. Additionally, the study proposes a high availability distributed systems architected integrated with CDN for ensuring the availability of information and information systems as presented in Figure 5.4 in Section 5.2.3. Mechanisms for assessing and identifying security measures for ensuring confidentiality, integrity and availability has been established and integrated into the developed framework for enhancing the security of information systems (Section 5.4.2).

Research Question 2: To what extents are the existing security controls ensure the security of information in information systems?

Response: Based on a literature review in Chapter 2, Research Methodology in Chapter 3, Research Findings in Chapter 4 and Discussion of the Results in Chapter 5; the study assessed the existing security controls in IS, a case study of education sector in Tanzania (Section 4.3, Section 4.4 and Section 5.3). The study found that the existing security controls are inadequate for ensuring the security of information in information systems as presented in Section 4.3, Section 4.4 and Section 5.3. The study assessed and identified security controls as summarized in Table 5.4 in Section 5.3. It has been incorporated into the developed framework for enhancing the security of information systems in Section 5.4.2.

Research Question 3: How to develop a framework for enhancing the security of information systems?

Response: Based on a Literature review in Chapter 2, Research methodology in Chapter 3, Findings in Chapter 4, Discussion of the results in Chapter 5; study assessed the security maturity level for the security of information systems, a case study of the education sector in Tanzania. In this assessment, it identified security requirements gap (security measures and security controls) using ISO/IEC 21827: Systems Security Engineering-Capability Maturity Model (SSE-CMM) as presented in section 4.5 and 5.4. The study It developed a framework for enhancing the security of information systems (Section 5.4). The framework was developed based on addressing the identified research gap in the literature review (chapter 2); using the findings of the results in Chapter 4, discussion of results in Chapter 5 and the established requirements in Section 5.4.1 for developing the framework for enhancing the security of information systems. These were all fused together by employing soft design science (SSM integrated with DSR) in a systematic circular iterative fashion until an optimal framework was obtained as presented in Section 5.4.2. The developed framework was validated using cryptographic algorithm based techniques (Section 5.6) and it was evaluated (Section 5.7).

Research Question 4: How to validate the developed framework for enhancing the security of information systems?

Response: Based on research methodology in Chapter 3, and Section 5.6 the developed framework was validated using algorithm based techniques using controlled simulation experiment (Section 5.6.4). A prototype based on cryptographic techniques

algorithms was developed (Section 5.6.3) to validate the proof concept for the developed framework for enhancing the security of information systems (Section 5.4.2).

Research Question 5: How to evaluate the developed framework for enhancing the security of information systems?

Response: The study employed the Method Evaluation Model (MEM) for evaluating the developed framework for enhancing the security of information systems as presented in Section 5.7. The developed framework for enhancing the security of information systems was evaluated based on its performance using a controlled experiment (Section 5.6.4) simulation. Moreover, it was evaluated for users' perception of the developed framework through a simulation experiment (Section 5.1.2 to 5.1.4).

6.1.3 Research Contributions

The research study has addressed the research problem, the objectives of the research and it has filled in the identified research gap. The major contributions of this study can be summarized as follows:

- i. The study has contributed security requirements (security measures and security controls) for ensuring security goals (confidentiality, integrity and availability) during information states (capturing, processing, storage and transmission) in IS to the body of knowledge of information systems security using soft design science (SSM integrated with DRS)
- ii. The study has contributed empirical evidence on how to improve the security of

information systems during information states in information systems

- iii. The study extends the applicability of soft systems methodology integrated with design science research (termed as soft design science) to information systems security
- iv. The study contributes an authentication and authorization system architecture for ensuring confidentiality of information in information systems
- v. The study contributes a crypto system architecture for ensuring confidentiality of information in information systems
- vi. The study contributes a cryptographic systems architecture for enhancing the integrity of information and information systems
- vii. The study contributes a high availability distributed systems architecture integrated with CDN for ensuring the availability of information in information systems
- viii. The study developed a multilayered based framework for enhancing the security of information systems
- ix. The study developed an artifact for the human sensor web for crowd sourcing information related to security incidents management
- x. The study developed a cryptographic based algorithm for validating proof of concept on how to enhance the security of IS using the developed framework for enhancing the security of information systems. It developed a prototype to simulate the proposed cryptographic based algorithm to enhance the security of information in IS.

6.1.4 Limitations and Further Research Work

The research study work was limited to enhancing the security of information and information systems during information states (capturing, processing, storage and transmission) in information systems, a case study of the education sector in Tanzania. Further research work should be undertaken to develop a homomorphic cryptography based algorithm for privacy preserving for human sensor web for crowd sourcing information related to security incidents management from whistle blowers in a ubiquitous computing environment.

6.2 Recommendations

The problem of loss of confidentiality, integrity and availability of information in information systems can be addressed using the developed framework for enhancing the security of information systems. The study recommends the adoption of the framework for enhancing the security of information systems in the education sector in Tanzania. The study proposes further study work on the extension of the applicability of the developed framework for enhancing the security of information systems to other sectors different from the education sector. This enables the generalization of the results and its applicability of the developed framework for enhancing the security of information systems to other sectors different from the education sector.

REFERENCES

- Abelson, H., Anderson, R., Bellare, S. M., Benaloh, J., Blaze, M., Diffie, W., & Weitzner, D. J. (2015). *Computer Science and Artificial Intelligence Laboratory Technical Report: Mandating insecurity by requiring government access to all data and communications*. <http://doi.org/10.1093/cybsec/tyv009>.
- Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2017). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. Retrieved March 2, 2018, from <http://arxiv.org/abs/1704.03578>.
- Addy, D., & Bala, P. (2016). Physical access control based on biometrics and GSM. In 2016 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2016, 21-24 Sept. 2016, Jaipur, India (pp. 1995-2001). IEEE.
- Agrawal, V., Kotia, D., Moshirian, K., & Kim, M. (2018). Log-Based Cloud Monitoring System for OpenStack. 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService), 276-281.
- Aissaoui, K., Ait idar, H., Belhadaoui, H., & Rifi, M. (2017). Survey on data remanence in Cloud Computing environment. In 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), 19-20 April 2017, Fez, Morocco. IEEE.
- Alfawaz, S. M. (2011). *Information security management: A case study of an information security culture*. PhD Thesis. The Queensland University of Technology. Retrieved from <https://eprints.qut.edu.au/41777/1/>

Salahuddin_Alfawaz_Thesis.pdf.

- Alhanahnah, M., & Yan, Q. (2018). Towards Best Secure Coding Practice for Implementing SSL / TLS. In IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 15-19 April 2018, Honolulu, HI, USA (pp. 166). IEEE.
- Alhazmi, O. H. (2015). Computer-Aided Disaster Recovery Planning Tools (CADRP). *International Journal of Computer Science & Security (IJCSS)*, 9(3), 1326139.
- Alizai, Z. A., Tareen, N. F., & Jadoon, I. (2018). Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures. In 2018 International Conference on Applied and Engineering Mathematics (ICAEM), 4-5 September 2018, Taxila, Pakistan (pp. 1156119). IEEE.
- Alkudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information Security: A Review of Information Security Issues and Techniques. In 2nd International Conference on Computer Applications and Information Security, ICCAIS 2019, 1-3 May 2019, Riyadh, Saudi Arabia, Saudi Arabia, IEEE (pp. 166). IEEE.
- Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information Security Policies: A Review of Challenges and Influencing Factors. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 5-7 Dec. 2016, Barcelona, Spain (pp. 3526358). IEEE.
- Alshboul, A. (2010). Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks. *Communications of the IBIMA, 2010*, 169. <http://doi.org/10.5171/2010.486878>

- Alsmadi, I., & Alazzam, I. (2016). Websitesø input validation and input-misuse-based attacks. In Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016, 2-4 Aug. 2016, Amman, Jordan (pp. 113ó116). IEEE.
- Altaf, I., Ul Rashid, F., Dar, J. A., & Rafiq, M. (2016). Vulnerability assessment and patching management. In International Conference on Soft Computing Techniques and Implementations, ICSCTI 2015, 8-10 Oct. 2015, Faridabad, India (pp. 16ó21). IEEE.
- Anand, P., & Ryoo, J. (2017). Security Patterns As Architectural Solution - Mitigating Cross-Site Scripting Attacks in Web Applications. In 2017 International Conference on Software Security and Assurance (ICSSA), 24-25 July 2017, Montreal, QC, Canada (pp. 25ó31). IEEE.
- Aufa, F. J., Endroyono, & Affandi, A. (2018). Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm. In Proceedings - 2018 4th International Conference on Science and Technology, ICST 2018, 7-8 Aug. 2018, Yogyakarta, Indonesia (Vol. 1, pp. 165). IEEE.
- Awad, H. a H., & Battah, F. M. (2011). Enhancing Information Systems Security in Educational Organizations in KSA through proposing security model. *International Journal of Computer Science Issues*, 8(5), 354ó358.
- Ayyagari, R., & Tyks, J. (2012). Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education: Innovations in Practice*, 11, 85ó96.
- Bakari, J. K. (2007). *A Holistic Approach for Managing ICT Security in Non-*

- Commercial Organisations A Case Study in a Developing Country*. Phd Thesis. Stockholm University. Retrieved from <http://www.diva-portal.org/smash/get/diva2:197030/FULLTEXT01.pdf>
- Balamurugan, B., Shivitha, N. G., Monisha, V., & Saranya, V. (2015). A Honey Bee behaviour inspired novel Attribute-based access control using enhanced Bell-Lapadula model in cloud computing. In International Conference on Innovation Information in Computing Technologies, 19-20 Feb. 2015, Chennai, India. IEEE.
- Balliu, M. (2014). *Logics for Information Flow Security : From Specification to Verification Doctoral Thesis in Computer Science*. Stockholm. Retrieved from <https://www.diva-portal.org/smash/get/diva2:743274/FULLTEXT04.pdf>
- Balon, N., & Thabet, I. (2004). The Biba Security Model. Retrieved June 2, 2017, from http://nathanbalon.net/projects/cis576/Biba_Security.pdf
- Barker, K., & Morris, S. (2013). *CCNA Security 640-554* (3rd editio). Cisco Press, 800 East 96th Street, Indianapolis, IN 46240: Pearson Education, Inc.
- Baruah, N. (2013). System Diagnosis and Fault Tolerance for Distributed Computing System: A Review. *International Journal of Computer Science & Communication Networks*, 3(4), 2846295.
- Basden, A. (2003). Reflections on CATWOE, a Soft Systems Methodology Technique for Systems Designs. *Information Systems Journal*, 17(2), 556-73. Retrieved from <http://dx.doi.org/10.1023/B:SPAA.0000018903.18767.18>
- Baset, A. Z., & Denning, T. (2017). IDE Plugins for Detecting Input-Validation

- Vulnerabilities. In *2017 IEEE Security and Privacy Workshops (SPW)*, 25-25 May 2017, San Jose, CA, USA (pp. 1436146). IEEE.
- Baskerville, R., Pries-Heje, J., & Venable, J. (2009). Soft Design Science Methodology. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, May 07 - 08, 2009, Philadelphia, Pennsylvania (pp. 1611). ACM New York, NY, USA.
- Beaujean, A. A. (2013). Factor Analysis using R. *Practical Assessment, Research and Evaluation*, 18(4), 1611. Retrieved from <http://pareonline.net/pdf/v18n4.pdf>
- Beissel, S. (2014). Meeting Security and Compliance Requirements Efficiently With Tokenization. *ISACA Journal*, 1, 166.
- Bhosale, K. S., Nenova, M., & Iliev, G. (2018). The distributed denial of service attacks (DDoS) prevention mechanisms on application layer. In *2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, 18-20 Oct. 2017, Nis, Serbia (pp. 1366-139). IEEE.
- Bishop, M. (1995). Theft of information in the take-grant protection model. *Journal of Computer Security*, 3(4), 283-309.
- Bosworth, S., Kabay, M. ., & Whyne, E. (2014). *Computer Security Handbook* (6th Editio). John Wiley & Sons, Inc., Hoboken, New Jersey.
- Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 8(2), 27-40.
- Bragg, R., Ousley, M. R., & Strassberg, K. (2008). *The Complete Reference Network Security*. New Delhi, India: Tata McGraw-Hill Publishing Company Limited.

- Breithaupt, J., & Merkow, S. M. (2014). *Information Security Principles of Success*. (2nd Edition, Ed.). Pearson Education, Inc.
- Burton, I., & Straub, J. (2019). Autonomous distributed electronic warfare system of systems. In 2019 14th Annual Conference System of Systems Engineering, SoSE 2019, 19-22 May 2019, Anchorage, AK, USA, USA (pp. 966101). IEEE.
- Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. In Iberian Conference on Information Systems and Technologies, CISTI, 19-22 June 2019, Coimbra, Portugal, Portugal, IEEE (pp. 19622).
- Chand, O. N., & Mathivanan, S. (2016). A survey on resource inflated Denial of Service attack defense mechanisms. In 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 19-19 Nov. 2016, Coimbatore, India (pp. 164). IEEE.
- Chatfield, C. A. (2009). *Privacy and Security in Ubiquitous Computing : Service Delivery and Identity in Intelligent Environments*. PhD Thesis. Griffith University, Brisbane, Australia. Retrieved from https://www120.secure.griffith.edu.au/rch/file/7c430a8f-f18d-63cc-517f-a485409a3631/1/Chatfield_2010_02Thesis.pdf
- Chaula, J. A. (2006). *A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance*. PhD Thesis. Stockholm University. Retrieved from <http://scholar.gurance#1>
- Checkland, P. B. (1998). *Systems Thinking, Systems Practice*. John Wiley & Sons Ltd. ISBN 0-471-98606-2.
- Checkland, P. B., & Scholes, J. (1990). *Soft Systems Methodology in Action*. New

- York: New York, NY, USA: John Wiley & Sons, Inc. Retrieved from <http://dl.acm.org/citation.cfm?id=130360>
- Chen, L., & Chen, L. (2017). *Scholarship at UWindsor Security Management for The Internet of Things By*. The University of Windsor. Retrieved from <https://elk.adalidda.net/2017/08/Security-Management-for-IoT.pdf>
- Chernov, D., & Sychugov, A. (2019). Problems of information security and availability of automated process control systems. In 2019 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2019, 25-29 March 2019, Sochi, Russia, Russia (pp. 165). IEEE.
- Clark, D. D., & Wilson, D. R. (1987). A Comparison of Commercial and Military Computer Security Policies. In 1987 IEEE Symposium on Security and Privacy, 27-29 April 1987, Oakland, CA, USA, USA (pp. 184-194). IEEE.
- Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment*, 7(3), 309-319.
- Cleeff, A. van. (2015). *Physical and Digital Security Mechanisms: Properties, Combinations and Trade-offs*. PhD Thesis. The University of Twente. Retrieved from http://doc.utwente.nl/95959/1/thesis_A_van_Cleeff.pdf
- Cloudflare. (2019). Content delivery network (CDN). Retrieved September 24, 2019, from <https://www.cloudflare.com/learning/cdn/what-is-a-cdn/>
- Cohen, L., Manion, L., & Morrison, K. (2007). *Research methods in education. Professional Development in Education* (6th editio). 270 Madison Avenue, New York, NY 10016: Routledge is an imprint of the Taylor & Francis Group, an informa business.
- Cundill, G., Cumming, G. S., Biggs, D., & Fabricius, C. (2012). *Soft Systems*

- Thinking and Social Learning for Adaptive Management. *US National Library of Medicine National Institutes of Health*, 1, 13620.
- Cunningham, M., & Cunningham, P. (2017). Report on ICT Initiatives and Research Capacity in IST-Africa Partner Countries. *ISTAfrica*, 1, 16380. Retrieved from http://www.ist-africa.org/home/files/IST-Africa_D2.1_ICTInitiatives_ResearchInnovationPriorities_v1_301017.pdf
- Davey, J. W., Gugiu, P. C., & Coryn, C. L. S. (2010). Quantitative Methods for Estimating the Reliability of Qualitative Data. *Journal of MultiDisciplinary Evaluation*, 6(13), 1406162.
- Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Management. The Sloan School of Management.
- DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems*, 19(4), 9630.
- Demesie Yalew, S., Mendonca, P., Maguire, G. Q., Haridi, S., & Correia, M. (2017). TruApp: A TrustZone-based authenticity detection service for mobile apps. In International Conference on Wireless and Mobile Computing, Networking and Communications, 9-11 Oct. 2017, Rome, Italy (Vol. 2017-October, pp. 169). IEEE.
- Dong, Q., Huang, D., Luo, J., & Kang, M. (2018). Achieving Fine-Grained Access Control with Discretionary User Revocation over Cloud Data. In 2018 IEEE Conference on Communications and Network Security (CNS), 30 May-1 June 2018, Beijing, China (pp. 169).

- Drago, A. (2015). *Methods and Techniques for Enhancing Physical Security of Critical Infrastructures*. PhD Thesis. University of Naples "Federico II". Retrieved from <http://www.fedoa.unina.it/10532/1/PhDThesisAnnaritaDrago.pdf>
- Drost, E. A. (2011). Validity and Reliability in Social Science Research. *Education Research and Perspectives*, 38(1), 105-123.
- Educause.edu. (2015). Higher Education Information Security Assessment Tool (HEIS Tool). net.educause.edu. Retrieved from <https://net.educause.edu/ir/library/excel/HEISCtool.xlsm>
- Ekstedt, M., Verno, A., & Lagerstrom, R. (2017). Analyzing the Effectiveness of Attack Countermeasures in a SCADA System. In *Proceeding CPSR-SG17 Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, Pittsburgh, PA, USA - April 18 - 21, 2017* ACM New York, NY, USA (pp. 73-78).
- Elias, M. (2015). *Design of Business Process Model Repositories Requirements, Semantic Annotation Model and Relationship Meta-model*. PhD Thesis. Stockholm University. Retrieved from <http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-117035>
- Elkamchouchi, H. M. (2018). An Advanced Hybrid Technique for Digital Signature Scheme. In *2018 5th International Conference on Electrical and Electronic Engineering (ICEEE)*, 3-5 May 2018, Istanbul, Turkey (pp. 375-379). IEEE.
- Farag, M. M., Azab, M., & Mokhtar, B. (2014). Cross-layer security framework for smart grid: Physical security layer. *IEEE PES Innovative Smart Grid*

Technologies, Europe, 167.

Farrell, R., & Hooker, C. (2013). Design, science and wicked problems. *Design Studies*, 34(6), 681-6705.

Fernando, M. S. (2018). IT disaster recovery system to ensure the business continuity of an organization. In 2017 National Information Technology Conference, NITC 2017, 14-15 Sept. 2017, Colombo, Sri Lanka (pp. 466-48). IEEE.

Fox, J. (2015). Introduction to the R Statistical Computing Environment. Retrieved June 9, 2016, from <http://socserv.socsci.mcmaster.ca/jfox/Courses/R/ICPSR/>

Fundo, A., Hysi, A., & Tafa, I. (2014). Secure Deletion of Data from SSD. (*IJACSA International Journal of Advanced Computer Science and Applications*, 5(8), 131-134.

Futcher, L. (2011). *An Integrated Risk-Based Approach to Support IT, Undergraduate Students, in Secure Software Development*. Retrieved from <http://dspace.nmmu.ac.za:8080/jspui/handle/10948/1673>

Gangire, Y., Da Veiga, A., & Herselman, M. (2019). A conceptual model of information security compliant behaviour based on the self-determination theory. In 2019 Conference on Information Communications Technology and Society, ICTAS 2019, 6-8 March 2019, Durban, South Africa, South Africa, IEEE (pp. 166). IEEE.

Gentry, C., & Halevi, S. (2011). Implementing Gentry's fully-homomorphic encryption scheme. In Paterson K.G. (eds) *Advances in Cryptology - EUROCRYPT 2011*. EUROCRYPT 2011. Lecture Notes in Computer

Science, vol 6632 (pp. 1629). Springer, Berlin, Heidelberg.
http://doi.org/10.1007/978-3-642-20465-4_9

Ghotbi, A., & Gharechedaghi, N. N. (2012). Evaluating the Security Actions of Information Security Management System in the Electronic Stock Commerce, and Providing the Improvement Strategies, 2(3), 304663053.

Gligoroski, D., Markovski, S., & Kocarev, L. (2013). Edon-R, an infinite family of cryptographic hash functions. *International Journal of Network Security*, 8(3), 2936300.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4), 5976607.

Golaghazadeh, F., Coulombe, S., Coudoux, F. X., & Corlay, P. (2018). Checksum-Filtered List Decoding Applied to H.264 and H.265 Video Error Correction. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(8), 199362006.

Gomes, P., Cadete, G., & Silva, M. M. da. (2017). Using Enterprise Architecture to Assist Business Continuity Planning in Large Public Organizations. In 2017 IEEE 19th Conference on Business Informatics (CBI), 24-27 July 2017, Thessaloniki, Greece (pp. 70678). IEEE.

Goyal, P., & Goyal, A. (2017). Comparative Study of two Most Popular Packet Sniffing Tools- Tcpdump and Wireshark. In 2017 9th International Conference on Computational Intelligence and Communication Networks, 16-17 Sept. 2017, Girne, Cyprus (pp. 77681). IEEE.

Graham, W. (1989). Action and Research: A Soft Systems approach to Organisational Development Evaluating Soft Systems & Organisational

- Development. Retrieved September 15, 2017, from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.453.4541&rep=rep1&type=pdf>
- Green, H. E. (2014). Use of theoretical and conceptual frameworks in qualitative research. *Nurse Researcher*, *21*(6), 34638.
- Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 3376355.
- Guelcher, L. A. (2015). *Vulnerability Assessment: Publicizing Top Secret / Special Compartmentalized Information Clearances on Social Media Sites and Its Impact on Organizational Cyber Security*. Mercyhurst University. Retrieved from <https://www.mercyhurst.edu/sites/default/files/uploads/804022-guelcher-thesis-final.pdf>
- Guernic, G. Le. (2007). *Confidentiality Enforcement Using Dynamic Information Flow Analyses*. Kansas State University. Retrieved from https://tel.archives-ouvertes.fr/tel-00198621/PDF/thesis_report.pdf
- Haynes, S. N., Richard, D. C. S., & Kubany, E. S. (1995). Content Validity in Psychological Assessment: A Functional Approach to Concepts and Methods Introduction to Content Validity. *Psychological Assessment*, *7*(3), 2386247.
- Hermawan, T., & Wardhani, R. W. (2017). Implementation AES with digital signature for secure web-based electronic archive. In 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), 5-6 Oct. 2016, Yogyakarta, Indonesia (pp. 166). IEEE.
- Hevner, A. R. (2007). A Three Cycle View of Design Science Research A Three

- Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, 19(2), 87692.
- Hevner, A. R., & Chatterjee, S. (2012). *Design Research in Information Systems: Theory and Practice*. (U. Ramesh Sharda Oklahoma State University, Stillwater, Ed.), *Springer (Integrated, Vol. 28)*. Springer.
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 756105.
- Huang, L. (2015). *Information security management*. Thesis. The Lapland University of Applied Sciences. Retrieved from https://www.theseus.fi/bitstream/handle/10024/87055/Huang_Lu.pdf?sequence=1
- Hussain, I., Negi, M. C., & Pandey, N. (2019). 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 29-31 August 2018, Noida, India, India. In 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 7096713). IEEE.
- ISACA. (2009). An Introduction to the Business Model for Information Security. *ISACA Journal*, 1(1), 1628.
- ISACA. (2012). COBIT 5 for Information Security. *ISACA Journal*, 1. Retrieved from <http://www.isaca.org/cobit/pages/info-sec.aspx>
- ISACA. (2016). State of Cybersecurity : Implications for 2016. *ISACA Journal*, 16 23. Retrieved from <http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2016.aspx>

- Ismail, Z., Masrom, M., Sidek, Z., & Hamzah, D. (2010). Framework to Manage Information Security for Malaysian Academic Environment. *Journal of Information Assurance & Cybersecurity*, 2010, 1616.
- ISO/IEC. (2016). ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management. Retrieved June 6, 2016, from <http://www.iso27001security.com/html/27035.html>
- ISO/IEC 21827. (2008). ISO/IEC 21827:2008 Information technology Security techniques - Systems Security Engineering Capability Maturity Model(SSE-CMM). Retrieved July 20, 2017, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=44716
- ISO/IEC 27001:2013. (2013). *ISO/IEC 27001:2013 Information technology Security techniques Information security management systems Requirements*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=54534
- ISO/IEC 27002:2013. (2013). *ISO/IEC 27002:2013 Information technology Security techniques Code of practice for information security controls*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=54533
- ITNEWSAFRICA.COM. (2017). Tanzanian government introduces secondary school ICT initiative. Retrieved March 21, 2018, from <http://www.itnewsafrika.com/2017/10/tanzanian-government-introduces-secondary-school-ict-initiative/>
- Jamiiforums. (2017). Hackers wafanya yao website ya UDSM. Retrieved March 1, 2018, from <https://www.jamiiforums.com/threads/hackers-wafanya-yao-website-ya-udsm.1341730/page-4>
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity.

Journal of Computer and System Sciences, 80(5), 9736993.

- Jerschow, Y. I. (2012). *Attackers, Packets, and Puzzles On Denial-of-Service Prevention in Local Area Networks*. PhD Thesis. der Heinrich-Heine-Universit. Retrieved from <https://pdfs.semanticscholar.org/62ee/610e145407a4d35a210e2a9d76015a6eddba.pdf>
- Jillepalli, A. A., Sheldon, F. T., Leon, D. C. De, Haney, M., & Abercrombie, R. K. (2017). Security Management of Cyber Physical Control Systems Using NIST SP 800-82r2. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*, 26-30 June 2017, Valencia, Spain (pp. 186461870). Valencia, Spain, Spain: IEEE.
- Jimenez, de R. E. L. (2016). Pentesting on web applications using ethical - hacking, 9-11 Nov. 2016, San Jose, Costa Rica. In *2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI)* (pp. 166). IEEE.
- Johansson, D. (2014). *Two Shades of Service Mobility: Application Mobility and Mobile E-services*. PhD Thesis. The Lulea University of Technology. Retrieved from <https://www.diva-portal.org/smash/get/diva2:990958/FULLTEXT01.pdf>
- Jones, J., Petruso, M., Williams, L., & Singh, M. P. (2017). How Good is a Security Policy against Real Breaches ? A HIPAA Case Study. In *2017 IEEE/ACM 39th International Conference on Software Engineering How* (pp. 5306 540).
- Joshi, M., Mittal, S., Joshi, K. P., & Finin, T. (2017). Semantically Rich, Oblivious Access Control Using ABAC for Secure Cloud Storage. In *2017 IEEE*

- International Conference on Edge Computing (EDGE), 25-30 June 2017, Honolulu, HI, USA (pp. 1426149). IEEE.
- Kaczmarczyk, M. (2015). *Fragmentation in storage systems with duplicate elimination*. PhD Dissertation. The University of Warsaw. Retrieved from <https://pdfs.semanticscholar.org/c778/032b2d5412436c61edfad76940c7e85be83a.pdf>
- Kane, M. T. (2001). Current Concerns in Validity Theory. *Journal of Educational Measurement*, 38(4), 3196342.
- Kanure, H. V, Ambawale, J. H., & Chougale, S. S. (2014). Web Application Scanning and Identification of Vulnerabilities for Different Attacks. *Int. Journal of Engineering Research and Applications*, 4(5), 1036106.
- Karokola, G. (2012). *A Framework for Securing e-Government Services The Case of Tanzania*. PhD Thesis. Stockholm University. Retrieved from <http://www.diva-portal.org/smash/get/diva2:557279/FULLTEXT04.pdf>
- Karokola, G., Kowalski, S., & Yngström, L. (2013). Evaluating a framework for securing e-government services - A case of Tanzania. In 2013 46th Hawaii International Conference on System Sciences, 7-10 Jan. 2013, Wailea, Maui, HI, USA (pp. 179261801). IEEE.
- Kasita, C., & Laizer, L. S. (2013). Security Architecture for Tanzania Higher Learning Institutions. *Data Warehouse*, 3(10), 25632.
- Kaspersky. (2017). The State of Industrial Cybersecurity 2017. Retrieved December 22, 2017, from [http://go.kaspersky.com/rs/802-IJN-240/images/ICS WHITE PAPER.pdf](http://go.kaspersky.com/rs/802-IJN-240/images/ICS_WHITE_PAPER.pdf)
- Kessler, G. C. (2019). An Overview of Cryptography. Retrieved September 7, 2019,

from <https://www.garykessler.net/library/crypto.html#types>

- Khan, W. Z., Khan, M. K., Bin Muhaya, F. T., Aalsalem, M. Y., & Chao, H. C. (2015). A Comprehensive Study of Email Spam Botnet Detection. *IEEE Communications Surveys and Tutorials*, 17(4), 227162295.
- Kimble, C. (2008). *Holistic Methodologies*. Retrieved from <http://www.chris-kimble.com/Courses/sdm/Presentations/SDM7.pdf>
- Kipanyula, M. J., Geoffrey, A. M., Fue, K. G., Mlozi, M. R. S., Tumbo, S. D., Haug, R., & Sanga, C. A. (2016). Web and Mobile Phone Based Rabies Surveillance System for Humans and Animals in Kilosa District, Tanzania. *International Journal of Information Communication Technologies and Human Development*, 8(2), 47659.
- Kissel, R., & Scholl, M. (2014). Guidelines for Media Sanitization. *National Institute of Standards and Technology(NIST)*, 800688(Revision 1), 1656. Retrieved from https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819
- Kitindi, E. J., Alex, A., Sanga, C., Shabani, A., Kibirige, G., Phillip, J., & Oketchi, J. (2014). Mobile phone based payment authentication system: An intervention for customers ø bank account fraud in Tanzania. *International Journal of Information and Communication Technology Research*, 4(9), 3256337. Retrieved from http://esjournals.org/journaloftechnology/archive/vol4no9/vol4no9_1.pdf
- Kolli, S., Lilly, J., & Wijesekera, D. (2018). Positive Train Control Security: An Intrusion-Detection System to Provide Cyber-Situational Awareness. *IEEE Vehicular Technology Magazine*, 13(3), 1613.

- Koo, J., Kim, Y. G., & Lee, S. H. (2019). Security Requirements for Cloud-based C4I Security Architecture. In 2019 International Conference on Platform Technology and Service, PlatCon 2019 - Proceedings, 28-30 Jan. 2019, Jeju, Korea (South), Korea (South), IEEE (pp. 164). IEEE.
- Kothari, C. (2004). *Research Methodology: Methods & Techniques* (2nd ed.). New Delhi: New Age International (P) Limited, Publishers.
- Krutz, R. L., & Vines, R.. (2007). *The CISSP and CAP Prep Guide* (Platinum E). New Delhi: Wiley Publishing Inc.
- Lampson, B. W. (1974). Protection in Proc. In "Protection, " in Proc. Fifth Princeton Symposium on Information Sciences and Systems, Princeton University, March 1971, pp. 437-443, reprinted in Operating Systems Review, 8,1, January 1974 (pp. 18624). Princeton University.
- Lane, M. (2014). *The development of a carrying capacity assessment model for the Australian socio- environmental context*. PhD Thesis. The Queensland University of Technology. Retrieved from https://eprints.qut.edu.au/67485/1/Murray_Lane_Thesis.pdf.
- LaPadula, L. J., & Bell, D. E. (1996). MITRE Technical Report 2547, Volume II. *Journal of Computer Security*, 4(263), 2396263.
- Lawal, M. ., Sultan, M. A. B., & Shakiru, A. O. (2016). Systemic Literature Review on SQL Injection Attacks. *International Journal of Soft Computing*, 11(1), 26635. <http://doi.org/DOI: 10.3923/ijscmp.2016.26.35>
- Lin, T. Y. T. Y. (2015). Chinese wall security policies information flows in business cloud. In 2015 IEEE International Conference on Big Data (Big Data), 29 Oct.-1 Nov. 2015, Santa Clara, CA, USA (pp. 160361607). IEEE.

- Line, M. B. (2015). *Understanding Information Security Incident Management Practices a Case Study in the Electric Power Industry*. PhD Thesis. Norwegian University of Science and Technology. Retrieved from <https://brage.bibsys.no/xmlui/bitstream/id/384795/Line, Maria Bartnes.pdf>
- Liu, C. Z., & Kavakli, M. (2018). An Agent-Based Collaborative Information Processing System for Mixed Reality Applications ó Part A : Agent-Aware Computing. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), 31 May-2 June 2018, Wuhan, China, China (pp. 127361278). IEEE.
- Lubis, A. R., Fachrizal, F., & Lubis, M. (2018). Wireless Service at Public University : A Survey of Users Perception on Security Aspects. In *2018 International Conference on Information and Communications Technology (ICOIACT), 6-7 March 2018, Yogyakarta, Indonesia* (pp. 78683). IEEE.
- Lubua, E. W., & Maharaj, M. S. (2012). ICT Policy and e-Transparency in Tanzania. In *IST-Africa 2012 Conference Proceedings, 9-11, May, 2012, Dar es Salaam, Tanzania*.
- Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering. *Information Resources Management Journal*, 24(September), 168.
- Lupiana, D. (2008). *Development of a framework to leverage knowledge management systems to improve security awareness*. Dublin Institute of Technology, School of Computing. Msc. Dissertation. Dublin Institute of Technology. Retrieved from <https://arrow.dit.ie/cgi/viewcontent.cgi?article=1004&context=scschcomdis>.

- Maconachy, S., & Ragsdale, W. (2001). A Model for Information Assurance: An Integrated Approach. In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, US Military Academy, West Point, NY* (pp. 3086310).
- Mahimane, A. (2013). *Effective Capacity Planning of the Virtual Environment using Enterprise Architecture*. Master Thesis. The Ohio State University. Retrieved from https://etd.ohiolink.edu/rws_etd/document/get/osu1367278818/inline.
- Mahundu, F. G. (2015). *E-Governance in the Public Sector: A Case Study of the Central Admission System in Tanzania*. PhD Thesis. Rhodes University. Retrieved from <http://contentpro.seals.ac.za/iii/cpro/DigitalItemViewPage.external?lang=eng&sp=1020845&sp=T&suite=def>.
- Mahundu, F. G. (2016). E-Governance: A Sociological Case Study of the Central Admission System in Tanzania. *The Electronic Journal of Information Systems in Developing Countries*, 79(6), 1611.
- Maranguni, N., & Grani, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society*, 14(1), 81695.
- Martínez, J., Rodríguez-molina, J., Castillejo, P., & Diego, R. De. (2013). Middleware Architectures for the Smart Grid: Survey and Challenges in the Foreseeable Future. *Energies*, 6(7), 359363621.
- Mbowe, J. E., Msanjila, S. S., Oreku, G. S., & Kalegele, K. (2016). On Development of Platform for Organization Security Threat Analytics and Management (POSTAM) Using Rule-Based Approach. *Journal of Software Engineering*

and Applications, 09(12), 6016623.

- McCumber, C. J. R. (1991). Information Systems Security: a Comprehensive Model. In The 14th National Computer Security Conference, October 1-4, 1991, Omni Shoreham Hotel Washington, D.C (pp. 3286337).
- MEST. (2016). Ministry of Education, Science and Technology (MEST). Retrieved May 2, 2018, from <http://moe.go.tz/en/>
- Mgaya, K. (2010). Development of information technology in Tanzania. Retrieved March 8, 2018, from <http://archive.unu.edu/unupress/unupbooks/uu19ie/uu19ie0i.htm>.
- Microsoft. (2002). The STRIDE Threat Model. Retrieved January 2, 2017, from [https://msdn.microsoft.com/en-us/library/ee823878\(v=cs.20\).aspx](https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx)
- Mikulcak, M., Herber, P., Gothel, T., & Glesner, S. (2018). Information flow analysis of combined simulink/stateflow models. In 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 27-29 June 2018, Paris, France (pp. 2296234). IEEE.
- Mirza, A. N. (2016). *Analyzing error detection performance of checksums in embedded networks*. Master Thesis. Strathmore University. Retrieved from <http://su-plus.strathmore.edu/handle/11071/4844>.
- MITRE. (2014). Heartbleed Bug: CVE-2014-0160. Retrieved July 20, 2017, from <https://nvd.nist.gov/vuln/detail/CVE-2014-0160>
- Mkansi, M., & Acheampong, E. A. (2012). Research philosophy debates and classifications: Studentsødilemma. *Electronic Journal of Business Research Methods*, 10(2), 1326140. <http://doi.org/1477-7029>.

- Moh.go.tz. (2016). Ministry of Health, Community Development, Gender, Elderly and Children. Retrieved May 10, 2017, from <http://moh.go.tz/en/>
- Moody, D. L. (2003). The Method Evaluation Model: A Theoretical Model for Validating Information Systems Design Methods. In Conference: Proceedings of the 11th European Conference on Information Systems, ECIS 2003, Naples, Italy 16-21 June 2003 (pp. 1327-1336).
- Mseteka, L., Phiri, J., & Tembo, S. (2019). Web and Mobile Examination Results Dissemination and Verification System Using Encryption and Cryptographic Hash Functions : A Case of TEVETA. *International Journal of Future Computer and Communication*, 8(1), 166-23.
- Mshangi, M., Nfuka, E. N., & Sanga, C. (2015). Using Soft Systems Methodology and Activity Theory to Exploit Security of Web Applications against Heartbleed Vulnerability. *International Journal of Computing and ICT Research*, 8(2), 326-52.
- Mshangi, M., Nfuka, E. N., & Sanga, C. (2016). Designing Secure Web and Mobile-Based Information System for Dissemination of Students Examination Results : The Suitability of Soft Design Science Methodology. *International Journal of Computing and ICT Research*, 10(2), 106-40.
- Mshangi, M., Nfuka, E. N., & Sanga, C. (2017). An Innovative Soft Design Science Methodology for Improving Development of a Secure Information System in Tanzania Using Multi-Layered Approach. *Journal of Information Security*, 8(3), 141-165.
- Mshangi, M., Nfuka, E. N., & Sanga, C. (2018). Human Sensor Web Crowdsourcing Security Incidents Management Platform. *Journal of Information Security*,

9(3), 1916208.

Mumtaz, N. (2015). Analysis of information security through asset management in academic institutes of Pakistan. In *2015 International Conference on Information and Communication Technologies (ICICT), 12-13 Dec. 2015, Karachi, Pakistan* (pp. 164).

Mwananchi. (2017). Wahalifu wa kimtandao wavamia tovuti ya Chuo Kikuu Huria. Retrieved October 26, 2017, from <http://www.mwananchi.co.tz/habari/Wahalifu--wa--kimtandao--wazua--taharuki--Chuo--Kikuu--Huria/1597578-4155850-11qoy91z/index.html>

Nabeel, M. (2017). The Many Faces of End-to-End Encryption and Their Security Analysis. In *2017 IEEE International Conference on Edge Computing (EDGE), 25-30 June 2017, Honolulu, HI, USA* (pp. 2526259). IEEE.

Nachtigal, S. (2009). *E-business Information Systems Security Design Paradigm and Model*. PhD Thesis. The University of London. Retrieved from <http://digirep.rhul.ac.uk/items/bf2711d5-4654-40ee-b1c6-4b4f0f83ac97/1/>

Navarro-Machuca, J., & Chen, L. C. (2016). Embedding Model-Based Security Policies in Software Development. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 9-10 April 2016* (pp. 1166122). IEEE.

NECTA. (2019). NECTA API. Retrieved November 19, 2019, from <https://api.necta.go.tz/>

Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). The Rapid Growth of Cybercrimes

- Affecting Information Systems in the Global : Is this a Myth or Reality in Tanzania ? *International Journal of Information Security Science*, 3(2), 1826199.
- Nilsen, P. (2015). Making sense of implementation theories, models and frameworks. *Implementation Science*, 10(1), 53. <http://doi.org/10.1186/s13012-015-0242-0>
- NIST. (2012). Guide for conducting risk assessments. *NIST Special Publication*, 800630(1), 1623. <http://doi.org/10.6028/NIST.SP.800-30r1>
- Novani, S., Putro, U. S., & Hermawan, P. (2014). An Application of Soft System Methodology in Batik Industrial Cluster Solo by Using Service System Science Perspective. *Procedia - Social and Behavioral Sciences*, 115(21 February 2014), 3246331.
- NSTISS. (1994). *National Training Standard for Information Systems Security (Infosec) Professionals*. Retrieved from http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf
- Nyantiga, Sicato, Rathore, Sung, & Park. (2019). Blockchain-Based Secure Storage Management with Edge Computing for IoT. *Electronics*, 8(8), 1622.
- OMNISECU. (2017). Types of Network Attacks against Confidentiality, Integrity and Avilability. Retrieved May 20, 2018, from <http://www.omnisecu.com/ccna-security/types-of-network-attacks.php>
- Onica, E., Ioan, A., Felber, P., Mercier, H., & Riviere, E. (2016). Confidentiality-Preserving Publish/Subscribe: A Survey. *ACM Computing Surveys (CSUR)*, 49(2), 1643.
- Otero, A. R. (2014). *An Information Security Control Assessment Methodology for*

- Organizations*. PhD Thesis. The Nova Southeastern University: College of Engineering and Computing. Retrieved from https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1265&context=gscis_etd
- Othman, M., Hassan, W. H., & Abdalla, A. H. (2007). Developing a secure mechanism for Bluetooth-based Wireless Personal Area Networks (WPANs). In 2007 International Conference on Electrical Engineering, 11-12 April 2007, Lahore, Pakistan (pp. 164). IEEE.
- OWASP. (2017). OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. Retrieved July 7, 2018, from https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Pan, J.-N., & Chen, S.-C. (2012). A new approach for assessing the correlated risk. *Industrial Management & Data Systems*, 112, 134861365.
- PCI-DSS. (2016). *Data Security Standard. Security*. Retrieved from https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf
- Peffer, K. E. N., Rothenberger, M., & Kuechler, B. (2012). Design Science Research in Information Systems Advances in Theory and Practice. In 7th International Conference, DESRIST 2012 Las Vegas, NV, USA, May 2012 Proceedings.
- PMO-RALG. (2016). The Prime Minister's Office, Regional Administration and Local Government (PMO-RALG). Retrieved May 28, 2016, from <http://www.tamisemi.go.tz/>
- PORALG. (2016). President's Office Regional Administration and Local Government (PORALG). Retrieved February 2, 2018, from <http://tamisemi.go.tz/>

- Promyslov, V. G. (2017). Assessment of the security architecture of control system using discretionary security models. In 2017 Tenth International Conference Management of Large-Scale System Development (MLSD), 2-4 Oct. 2017, Moscow, Russia (pp. 164). IEEE.
- Purcell, E. J. (2015). *Defining and Understanding Security in the Software Development Life Cycle. Technical Report*. Retrieved from <https://buildsecurityin.us-cert.gov/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes>
- Qadir, S., & Quadri, S. M. K. (2016). Information Availability : An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, 7(April), 1856194.
- Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2018). Decrypting SSL / TLS Traffic for Hidden Threats Detection. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, Ukraine, 24-27 May 2018 (pp. 1436146). IEEE.
- Razali, S. (2018). Evaluation of Methodö as IT Artifacts in Soft Design Science Research: Development of Community Based E-Museum Framework Towards Sustainable Cultural Heritage Information System. In Rocha Á., Adeli H., Reis L.P., Costanzo S. (eds) Trends and Advances in Information Systems and Technologies. WorldCISTø18 2018. Advances in Intelligent Systems and Computing, vol 745. Springer, Cham (pp. 9156924). Springer International Publishing.
- Razali, S., Noor, N. L. M., & Adnan, W. A. W. (2010). Applying Soft System

Methodology (SSM) into the design science: Conceptual modeling of community based E-museum (ComE) framework. Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, 27016-2707.

REUTERS. (2014). Edward Snowden: Leaks that exposed US spy programme. Retrieved April 6, 2014, from <http://www.bbc.com/news/world-us-canada-23123964>

Rezaeighaleh, H., Laurens, R., Zou, C. C., & Model, A. T. (2018). Secure Smart Card Signing with Time-based Digital Signature. In 2018 International Conference on Computing, Networking and Communications (ICNC), 5-8 March 2018, Maui, HI, USA (pp. 1826-187). IEEE.

Rizk, D., Rizk, R., & Hsu, S. (2019). Applied layered-security model to IoMT. In 2019 IEEE International Conference on Intelligence and Security Informatics, ISI 2019, 1-3 July 2019, Shenzhen, China, China, IEEE (p. 227). IEEE.

Robert, E., & Hemalatha, M. (2013). Efficient malware detection and tracer design for operating system. *Research Journal of Applied Sciences, Engineering and Technology*, 6(11), 20526-2060.

Roessing, R. M. von. (2010). The Business Model for Information Security. *ISACA Journal*, 1627. Retrieved from <https://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>

Rudman, L. (2014). Analysis of Ntp Based Amplification Ddos Attacks Submitted in partial fulfillment. Thesis. Grahamstown: Rhodes University.

Rupere, T., Mary, M., & Zanamwe, N. (2012). Towards Minimizing Human Factors

- In End-User Information Security. *International Journal of Computer Science and Network Security*, 12(12), 1596167.
- Sabena, D. (2015). *New Test and Fault Tolerance Techniques for Reliability Characterization of Parallel and Reconfigurable Processors*. PhD Thesis. Politecnico Di Torino. Retrieved from http://www.phd-dauin.polito.it/pdfs/Daive SABENA_thesis.pdf
- Salner, M., & Ph, D. (1999). Beyond Checkland & Scholes: Improving SSM. Retrieved January 5, 2018, from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.619.4939&rep=rep1&type=pdf>
- Sanga, C. (2010). *A Technique for the Evaluation of Free and Open Sources E-learning Systems*. PhD Thesis. The University of the Western Cape. Retrieved from; http://etd.uwc.ac.za/xmlui/bitstream/handle/11394/2564/Sanga_PHD_2010.pdf?sequence=1.
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. (5th edition, Ed.). England: Pearson Education Limited.
- Schultz, D. A. (2012). *Decentralized Information Flow Control for Databases*. PhD Thesis. Massachusetts Institute of Technology. Retrieved from <http://pmg.csail.mit.edu/papers/das-phd.pdf>.
- Sensuse, D. I., & Ramadhan, A. (2012). Enriching Soft Systems Methodology (SSM) with Hermeneutic in E-Government systems development process. *International Journal of Computer Science Issues*, 9(1), 17623.
- Shaaban, H. K. (2014). *Enhancing the Governance of Information Security in*

- Developing Countries: The Case of Zanzibar*. PhD Thesis. Bedfordshire.
Retrieved from <http://uobrep.openrepository.com/uobrep/bitstream/10547/315359/1/Hussein-Shaabab-PhD-Thesis.pdf>
- Shamala, P., & Ahmad, R. (2014). A proposed taxonomy of assets for information security risk assessment (ISRA). In 2014 4th World Congress on Information and Communication Technologies, WICT 2014, 8-11 Dec. 2014, Bandar Hilir, Malaysia (pp. 29633). IEEE.
- Shamsi, J. A., & Khojaye, M. A. (2018). Understanding privacy violations in big data systems. *IT Professional*, 20(3), 73681.
- Sharma, D. (2016). Cryptography by reversal of speech signal elements and implementing checksum. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 16-18 March 2016, New Delhi, India (pp. 7256728).
- Sherwood, J., Clark, A., & Lynas, D. (2009). Enterprise Security Architecture. *SABSA White Paper*, 6(4), 43654.
<http://doi.org/10.1080/10658989809342548>
- Shiaeles, S. (2013). *Real time detection and response of distributed denial of service attacks for web services by*. The Democritus University of Thrace.
Retrieved from [https://www.infosec.aueb.gr/Publications/PhD thesis Shiaeles DUTH.pdf](https://www.infosec.aueb.gr/Publications/PhD%20thesis%20Shiaeles%20DUTH.pdf)
- Smyth, D. S., & Checkland, P. B. (1976). Using a Systems Approach: The Structure of Root Definitions. *Journal of Applied Systems Analysis*, 5(1), 75683.
Retrieved August 21, 2018, from <http://clico.pl/services/practical-defense-in-depth-protection-against-botnets> Soltanmohammadi, S., Asadi, S., Ithnin, N., &

- Science, C. (2013). Main human factors affecting information system security Saeed. *Interdisciplinary Journal of Contemporary Research in Business*, 5, 3296354.
- Sood, A. K., & Enbody, R. J. (2011). Persistent Cross-interface Attacks. *ISACA Journal*, 6, 166.
- Straub, J. (2019). Cyber mutual assured destruction as a system of systems and the implications for system design. In 2019 14th Annual Conference System of Systems Engineering, SoSE 2019, 19-22 May 2019, Anchorage, AK, USA, USA (pp. 1376139). IEEE.
- Suhail, H. S. M., Mullapathi, S., & Ustun, T. S. (2019). Analysis and Implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security. *IEEE Access*, 7, 80980680984.
- Sultan, A., Yang, X., Hussain, S. B., & Hu, W. (2018). Physical -Layer Data Encryption using Chaotic Constellation Rotation in OFDM-PON. In 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 9-13 Jan. 2018, Islamabad, Pakistan (pp. 769). IEEE.
- Sun, G., Li, S., & Chen, X. (2019). Research on a component testing tool supporting data integrity verification. In 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analytics, ICCCBDA 2019, 12-15 April 2019, Chengdu, China, China (pp. 4776482). IEEE.
- Sur, E., & Yazici, Y. (2017). Design, Practice and Research : the Effects of Mobile and Web-. *Design, Practice and Research: The Effects of Mobile and Web-Based Learning Systems*, 5(1), 36647.

- Sviridov, A., Bobkov, V., Bobrikov, D., & Balashov, A. (2019). The concept of information security in the process control system. In Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus, 28-31.
- Symantec. (2016). Internet Security Threat Report. Retrieved May 20, 2017, from <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>
- Symantec. (2017). 2017 Internet Security Threat Report (pp. 1677). Retrieved from <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>
- Symantec. (2019). Internet Security Threat Report. Retrieved from [http://doi.org/10.1016/S1353-4858\(05\)00194-7](http://doi.org/10.1016/S1353-4858(05)00194-7)
- Talib, A. M. (2015). Ensuring Security, Confidentiality and Fine-Grained Data Access Control of Cloud Data Storage Implementation Environment. *Journal of Information Security*, 6, 1186130.
- Tambe, P., & Vora, D. (2016). Privacy preservation on social network using data sanitization. In 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 20-21 May 2016, Bangalore, India (pp. 7516753). IEEE.
- Tang, Z., Ding, X., Zhong, Y., Yang, L., & Li, K. (2018). A self-adaptive bell-lapadula model based on model training with historical access logs. *IEEE Transactions on Information Forensics and Security*, 13(8), 204762061.
- Tanovic, A., & Marjanovic, I. S. (2019). Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard,

- 20-24 May 2019, Opatija, Croatia, Croatia. In 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, *MIPRO 2019 - Proceedings* (pp. 150361508). IEEE.
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53655.
- Tayade, P. C., & Wadhe, A. P. (2014). Review Paper on Privacy Preservation through Phishing Email Filter. *International Journal of Engineering Trends and Technology (IJETT), 9*(12), 6006604.
- TCRA. (2017). *TCRA Quarterly Communications Statistics Report, March 2017*.
- Terblanché, J. R. (2013). *Legal risk and compliance risk in the banking industry in South Africa*. Potchefstroom Campus of the North-West University. Retrieved from; [http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1024.5377 &rep=rep1&type=pdf](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1024.5377&rep=rep1&type=pdf)
- Thatcher, R. W. (2010). Validity and Reliability of Quantitative Electroencephalography. *Journal of Neurotherapy, 14*(2), 1226152.
- THE CITIZEN. (2017). ICT school project launched. Retrieved March 21, 2018, from <http://www.thecitizen.co.tz/News/ICT--school--project--launched-secondary-kibaha/1840340-4137006-6jn1pgz/index.html>
- Tipton, H. F., & Krause, M. (2008). *Information Security Management Handbook - Volume 2* (6th Editio). Taylor & Francis Group, LLC.
- Toapanta, S. M. T., Salazar, C. E. S., Moran, D. H. P., Gallegos, L. E. M., & Del Rocio Maciel Arellano, M. (2019). Analysis of appropriate security processes to mitigate risk in a popular election system. In CITS 2019 -

Proceeding of the 2019 International Conference on Computer, Information and Telecommunication Systems, 28-31 Aug. 2019, Beijing, China, China (pp. 165).

Tsega, H., Lemmens, R., Kraak, M. J., & Lung, J. (2015). Towards a smarter system for Human Sensor Web. In *2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), 23-27 March 2015, St. Louis, MO, USA* (pp. 14619). IEEE.

Tsegaye, T., & Flowerday, S. (2014). Controls for Protecting Critical Information Infrastructure from Cyberattacks. In *World Congress on Internet Security (WorldCIS-2014), 8-10 Dec. 2014, London, UK* (pp. 24629). IEEE.

Uctu, G., Alkan, M., Dogru, I. A., & Dorterler, M. (2019). Perimeter Network Security Solutions: A Survey. In *3rd International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2019 - Proceedings, 11-13 Oct. 2019, Ankara, Turkey, Turkey, IEEE*. IEEE.

Unuakhalu, M. F., Sigdel, D., & Garikapati, M. (2014). Integrating Risk Management in System Development Life Cycle. *International Journal of Software and Web Sciences (IJSWS)*, 8(1), 169.

URT. (2003). *National Information and Communications Technologies Policy*. Retrieved from http://www.tanzania.go.tz/egov_uploads/documents/National ICT Policy of 2003_1.pdf

URT. (2007). Information & Communication Technology (ICT) Policy for Basic Education. Retrieved June 11, 2019, from <http://www.moe.go.tz/sw/machapisho/send/27-policy-sera/219-ict-policy-for-basic-education-2007.html>

- URT. (2015a). The Cybercrimes ACT, 2015. Retrieved June 1, 2019, from <https://www.tcra.go.tz/images/documents/policies/TheCyberCrimeAct2015.pdf>
- URT. (2015b). The Electronic Transactions Act, 2015. Retrieved August 8, 2018, from; <https://www.tcra.go.tz/images/documents/policies/TheElectronicTransactionAct.pdf>
- URT. (2016). Education. Retrieved January 5, 2016, from <http://tanzania.go.tz/home/pages/14>
- URT. (2017). National Information and Communications Technology Policy. Retrieved August 10, 2019, from <http://www.mwtc.go.tz/uploads/publications/en1490101734-National ICT Policy 2016.pdf>
- URT. (2019). Government e-Payment Gateway. Retrieved June 1, 2019, from <https://sp.gepg.go.tz/login>
- Varshney, G., Misra, M., & Atrey, P. (2018). A new secure authentication scheme for web login using BLE smart devices. In *2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, 27-29 Oct. 2017, Xiamen, China (Vol. 2017-October, pp. 956-98).
- Vemuri, S., Chala, S., & Fathi, M. (2017). Automated use case diagram generation from textual user requirement documents. Canadian Conference on Electrical and Computer Engineering, 30 April-3 May 2017, Windsor, ON, Canada, IEEE.
- Venter, I. M., Ponelis, S. R., & Renaud, K. V. (2015). Deploying Design Science Research in Graduate Computing Studies in South Africa Full Paper. In AIS

- Electronic Library (AISEL). Twenty First Americas Conference on Information Systems, Puerto Rico (pp. 1611).
- Verma, A., Guleria, D., & Lakhanpal, K. (2014). A Survey of Software Fault Tolerance, Reliability and Safety, 2(4), 465.
- Vijayasathya, R. (2012). *A Systems Approach to Network Modelling for DDoS Attack Detection using Naïve Bayes Classifier*. Indian Institute of technology. Retrieved from https://www.cse.iitm.ac.in/~ravi/papers/Vijayasathya_thesis.pdf.
- Wang, T., Liu, X., Li, S., Liao, X., Li, W., & Liao, Q. (2018). MisconfDoctor: Diagnosing misconfiguration via log-based configuration testing. In Proceedings - 2018 IEEE 18th International Conference on Software Quality, Reliability, and Security, QRS 2018, 16-20 July 2018, Lisbon, Portugal (pp. 1612). IEEE.
- Watkins, M., & Wallace, K. (2008). *CCNA Security Official Exam Certification Guide* (3rd Editio). Pearson Education, Inc. and Dorling Kindersley Publishing, Inc.
- Weerathunga, P. E., & Cioraca, A. (2016). The Importance of Testing Smart Grid IEDs against Security Vulnerabilities General Electric Grid Solutions - Canada. In 2016 69th Annual Conference for Protective Relay Engineers (CPRE), 4-7 April 2016, College Station, TX, USA (pp. 1621). IEEE.
- Whitmen, M. ., & Mattord, H. . (2012). *Principles of Information Security* (4th ed.). Boston, MA 02210, USA: Cengage Learning.
- Williams, B., & Hof, S. van . (2014). *Wicked Solutions A Systems Approach to Complex Problems*. Bob!Williams. Retrieved from

<http://www.bobwilliams.co.nz/wicked.pdf>

Yan, G., Yu-qing, Y., & Li-lei, L. (2011). Security engineering capability maturity model. *Elsevier*, 24, 335 ó 339.

Yonazi, J. (2012). Cyber Security in Tanzania. In Cyber Security in Tanzania: Report on from the Cyber-Security Mini-Conference, Dar es Salaam. Dar es Salaam. Retrieved from: http://www.academia.edu/1925835/Cyber_Security_in_Tanzania_Proceedings_of_the_Cyber_Security_Mini-Confrece.

Zhe, D., Qinghong, W., Naizheng, S., & Yuhan, Z. (2017). Study on Data Security Policy Based on Cloud Storage. In 2017 iee 3rd international conference on big data security on cloud (bigdatasecurity), iee international conference on high performance and smart computing (hpsc), and iee international conference on intelligent data and security (ids), 26-28 May 2017, (pp. 145ó149). IEEE.

APPENDICES

Appendix A: Research Access and Ethical Issues

A.1: Ethical Issues Addressed

The following form represents the research ethical form for ethical issues addressed.

THE OPEN UNIVERSITY OF TANZANIA

DIRECTORATE OF RESEARCH, PUBLICATIONS AND POSTGRADUATE STUDIES

P.O. Box 23409,
Dar es Salaam, Tanzania
<http://www.out.ac.tz>



Tel: 255-22-2666752/2668445 ext.2101;
E-mail: drpc@out.ac.tz

DECLARATION OF CONFIDENTIALITY

To: The Chief Executive Officer of (give the title of the Chief Executive Officer of the institution/firm/organization etc visiting)
I, (Name and Reg. no.), of the Department of, Faculty of, Open University of Tanzania, declare that, I will maintain secrecy and confidentiality, and will not use any data and information obtained from your organization in the course of my research for any purpose other than for my academic endeavors.

Signature, (student)

Date

Countersigned by:

Name (Supervisor)

Signature (Supervisor)

Date

A.2: Introduction Letters to Organisations

The following is the research clearance letter to introduce the researcher to organisations under study.

A.3: Research Permit from Regional Offices and Organisations

The following are samples of research permit from regional offices and organisations.

Appendix B: Data Collection Tools

B.1: Survey Questionnaire for Management Staff

THE OPEN UNIVERSITY OF TANZANIA
FACULTY OF SCIENCE, TECHNOLOGY AND ENVIRONMENTAL STUDIES



SURVEY QUESTIONNAIRE FOR MANAGEMENT STAFF

This study is seeking to explore the security requirements for Enhancing Security of Information Systems: Case of Tanzania Education Sector.

I am requesting you to take part in this research activity for Enhancing the Security of Information Systems in Tanzania Education Sector, by completing this short research survey questionnaire. Please *be honest* in completing this survey questionnaire. Please do not write your name. Please, if you wish to discuss any aspects of the review or this document do not hesitate to contact me.

STUDENT'S NAME

Maduhu Mshangi

Mobile: 0754-860027/0714-941746

E-mail: mshangimaduhu@yahoo.com/mshangimaduhu@necta.go.tz

SUPERVISORS

Dr. Edephonc Ngemera Nfuka (OUT)

Dr. Camilius Sanga, Full Professor (SUA)

B.2.Survey Questionnaire for Management Staff

OPEN UNIVERSITY OF TANZANIA
FACULTY OF SCIENCE, TECHNOLOGY AND ENVIRONMENTAL STUDIES

The aim of this questionnaire is to find out your feelings, perception and options on the Information Security/Information Systems Security.

Note: All information, including answers to various questions in this questionnaire, shall be treated as confidential and solely for academic purposes only. Respondents should feel free to express themselves openly. Please do not reveal your name in this questionnaire.

Part One: Personal Information

For the following statements please tick (✓) the box that matches your view most closely.

(For Organization Name, Other and occupation fill in accordingly).

1	Organization Name			
2	Gender	Male <input type="checkbox"/>	Female <input type="checkbox"/>	
3	Age	Below 25 Years <input type="checkbox"/>	25-35 Years <input type="checkbox"/>	36-45 Years <input type="checkbox"/>
		46-55 Years <input type="checkbox"/>	Above 55 Years <input type="checkbox"/>	
4	Level of Education	Postgraduate <input type="checkbox"/>	First Degree <input type="checkbox"/>	Advanced Diploma <input type="checkbox"/>
		Ordinary Diploma <input type="checkbox"/>	Other	
5	Occupation/Profession			

Part Two: Information Systems Security

For the following statements, please indicate your response by ticking (✓) one check box per question: **rating scale of 0-5: minimum 0 and maximum 5.**

0-Not performed (non-existent); 1-Performed informally (unplanned);

2-Partially implemented (planned);

3-Implementation is in progress (planned and tracked);

4-Fully implemented (well defined and auditable);

5-Fully implemented and regularly updated (monitored and audited for compliance).

i.	The organization has an information security policy that has been approved by the top management/board of directors	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ii.	The organization has an information security policy that has been published and communicated to all employees and relevant stakeholders	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iii.	Organization review the information security policy at defined intervals (every 1 year/2 year, etc.) to encompass significant change and monitor for compliance	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iv.	Organization perform screening/ background checks (vetting) of employees	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
v.	Organization conduct security awareness, training and education to employees	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vi.	The organization has risk register and, it is regularly reviewed and updated (every 1 year/2 years/3 years, etc.)	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vii.	The organization has an information security committee in place and is functional	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
viii.	The organization has staff assigned security responsibility and report to top management	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ix.	Organization has budget for information security program	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
x.	The organization has a documented business continuity plan for information technology that is based on a business impact analysis, is periodically tested, and has been reviewed and approved by top management or the board of trustees	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xi.	The organization has an incident response team in place and is functional	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xii.	Employees in Organization use physical key locks and smartcards/biometrics to access their offices	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>

Comments and Suggestions (if any)

--

Thanks you very much for your responses

B.3: Survey Questionnaire for General Staff

THE OPEN UNIVERSITY OF TANZANIA
FACULTY OF SCIENCE, TECHNOLOGY AND ENVIRONMENTAL STUDIES

The aim of this questionnaire is to find out your feelings, perception and options on
the Information security/IS security

Note: All information, including answers to various questions in this questionnaire, shall be treated as strictly confidential and solely for academic purposes only. Respondents should feel free to express themselves openly. Please do not reveal your name in this questionnaire.

Part One: Personal Information

(For the following statements please tick ν the box that matches your view most closely).

(For the location, Institution Name, Other and occupation fill in accordingly)

1	Institution Name			
2	Gender	Male <input type="checkbox"/>	Female <input type="checkbox"/>	
3	Age (Years) Ago	Below 25 Years <input type="checkbox"/>	25-35 Years <input type="checkbox"/>	36-45 Years <input type="checkbox"/>
		46-55 Years <input type="checkbox"/>	Above 55 Years <input type="checkbox"/>	
4	Level of Education	Postgraduate <input type="checkbox"/>	First Degree <input type="checkbox"/>	Adv. Diploma <input type="checkbox"/>
		Ordinary Diploma <input type="checkbox"/>	Other	
5	Occupation/Profession			

Part Two: IS Security

(For the following statements, please indicate your response: 0-Not performed (non-existent); 1-Performed informally (ad-hoc); 2-Partially implemented; 3-Close to completion; 4-Fully implemented; 5-Continuously improving (optimized) by ticking ν one check box per question).

Please indicate your response: 0-Not performed (non-existent); 1-Performed informally (ad-hoc); 2-Partially implemented; 3-Close to completion; 4-Fully implemented; 5-Continuously improving (optimized) by ticking ν one check box per question.							
1	There is information security policy in place	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
2	I have read the Information security policy	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
3	Information security policy is periodically reviewed	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
4	I have signed confidentiality or non-disclosure agreement for the protection of an organisation's information assets	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
5	There is a periodic awareness and training program in information security	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
6	There is a disciplinary action against the non-compliant employee to information security policy	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
7	I agreed and signed the terms and conditions of employment that includes responsibilities for information security.	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
8	I receive information security awareness training regularly	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
9	Access to my office is through a door that has a lock	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
10	I wear employee identity card all the time inside the organisation's building	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
11	There are rules for using IS, electronic mail and Internet	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
12	I do not share the password and I am the only person who knows my password for access to an organisation's IS.	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
13	My password contains alphabets and numbers, and it expires after a given period (less than 90 days).	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
14	I use encryption when sending sensitive information	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
15	My computer automatically set to lock automatically after a few minutes of idle time and require a password to unlock it.	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
16	I know where to report information security incidents (e.g. viruses, fire, flood, etc.)	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
17	I am aware of an organisation's business continuity plans	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
18	I am aware of the organisation's guidelines on retention and disposal of information	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>

Thanks you very much for your responses

B.4: Survey Questionnaire for IT Staff

OPEN UNIVERSITY OF TANZANIA
FACULTY OF SCIENCE, TECHNOLOGY AND ENVIRONMENTAL STUDIES

The aim of this questionnaire is to find out your feelings, perception and options on
the Information security/IS security

Note: All information, including answers to various questions in this questionnaire, shall be treated as strictly confidential and solely for academic purposes only. Respondents should feel free to express themselves openly. Please do not reveal your name in this questionnaire.

Part One: Personal Information

(For the following statements please tick ν the box that matches your view most closely).

(For the location, Institution Name, Other and occupation fill in accordingly)

1	Institution Name			
2	Gender	Male <input type="checkbox"/>	Female <input type="checkbox"/>	
3	Age (Years) Ago	Below 25 Years <input type="checkbox"/>	25-35 Years <input type="checkbox"/>	36-45 Years <input type="checkbox"/>
		46-55 Years <input type="checkbox"/>	Above 55 Years <input type="checkbox"/>	
4	Level of Education	Postgraduate <input type="checkbox"/>	First Degree <input type="checkbox"/>	Adv. Diploma <input type="checkbox"/>
		Ordinary Diploma <input type="checkbox"/>	Other	
5	Occupation/Profession			

Part Two: IS Security

(For the following statements, please indicate your response: 0-Not performed (non-existent); 1-Performed informally (ad-hoc); 2-Partially implemented; 3-Close to completion; 4-Fully implemented; 5-Continuously improving (optimized) by ticking ν one check box per question).

1. Unauthorised disclosure and access controls of information

Please indicate your response: 0-Not performed (non-existent); 1-Performed informally (ad-hoc); 2-Partially implemented; 3-Close to completion; 4-Fully implemented; 5-Continuously improving (optimized) by ticking ν one check box per question.							
i.	Does your institution use PIN or password for accessing data/information in an information system(s)?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ii.	Does your institution use smart or biometric (e.g. finger print) to access sensitive areas?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iii.	Does your institution encrypt data/information during transmission, storage and processing in IS?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iv.	Does your institution employ technologies to block or restrict unencrypted sensitive information from traveling to untrusted networks?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
v.	Does your institution have segmented network architecture to provide different levels of security based on the information's classification?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vi.	Are Internet-accessible servers protected by more than one security layer (firewalls, intrusion detection system (IDS), intrusion prevention system (IPS))	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vii.	Does your institution have classified the information resources (assets) by indicating access levels	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
viii.	Does your institution have a process for posture checking, such as current antivirus software (antimalware), firewall enabled, OS patch level, etc., of devices as they connect to your network?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ix.	Do all individuals interacting with organization systems receive information security awareness training?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
x.	Does your institution have a media-sanitization process that is applied to equipment prior to disposal, reuse, or release?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xi.	Does your institution have an access control mechanism (role based, user rights, access control lists) for authorizing and revoking access rights to IS?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xii.	Does your institution have a process for routinely monitoring logs to detect unauthorized and anomalous activities?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xiii.	Does your institution have a secure deletion process for sensitive data/information (files/folders) that is applied to equipment prior to disposal, reuse, or release?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>

2. Consistency, accuracy and trustworthiness of the information

Please indicate your response: 0-Not performed (non-existent); 1-Performed informally (ad-hoc); 2-Partially implemented; 3-Close to completion; 4-Fully implemented; 5-Continuously improving (optimized) by ticking \checkmark one check box per question.							
i.	Does your institution have procedures to regularly review users' access to ensure only needed privileges (need to know principle) are applied?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ii.	Does your institution use checksum (e.g. MD5, SHA3) for ensuring the integrity of data/information during storage, transmission and processing)?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iii.	Does your institution use a digital signature (non-repudiation) to guarantee the message sent is the message received (authenticity of information)?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iv.	Are changes to IS tested, authorized, and reported?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
v.	Are security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments automatically logged?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vi.	Does your institution have a configuration-management process in place to ensure that changes to your critical systems are for valid business reasons and have received proper authorization?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vii.	Are duties sufficiently segregated to ensure unintentional or unauthorized modification of information is detected?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
viii.	Does your institution practice job rotation to breaks up opportunities for collusion and fraudulent activities?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ix.	Are steps taken to secure log data to prevent unauthorized access and tampering?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
x.	Does your institution regularly review administrative and operative access to audit logs?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xi.	Does your institution have an audit trail(s) (audit log) for a sensitive information system(s) and it is periodically monitored?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xii.	Does your institution continuously monitor your wired and wireless networks for unauthorized access?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xiii.	Does your institution have integrity monitoring tool(s) for alerting personnel for unauthorized modification of critical system files, configuration files, or content files; and software configured to perform critical file(s) comparisons at least weakly?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>

3. Reliable and timely access to information

Please indicate your response: 0-Not performed (non-existent); 1-Performed informally (ad-hoc); 2-Partially implemented; 3-Close to completion; 4-Fully implemented; 5-Continuously improving (optimized) by ticking \surd one check box per question.							
i.	Does your institution have a documented business continuity plan for information technology that is based on a business impact analysis, is periodically tested and has been reviewed and approved by top management or the board of trustees?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ii.	Are incident-handling procedures in place to report and respond to security events throughout the incident life cycle, including the definition of roles and responsibilities?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iii.	Does the institution incident response team aware of legal or compliance requirements surrounding evidence collection?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iv.	Is your data backup process frequency consistent with the availability requirements of your organization?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
v.	Does your institution routinely test the restore procedures?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vi.	Does your institution have sufficient capacities (hardware, infrastructure, bandwidth, memory, etc.) to process all requests as quickly as necessary for an information system(s)?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vii.	Are the IS in the institution implemented with fault tolerance (hardware redundancy, software recovery) to continue with service(s) delivery in case of system (s) failure?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
viii.	Does your institution have system monitoring mechanisms to ensure continuous availability of information system(s)?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ix.	Does your institution have preventative measures in place to protect critical hardware and wiring from natural and man-made threats?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>

4. Safeguards/countermeasures to avoid or minimize/mitigate security risks

Please indicate your response: 0-Not performed (non-existent); 1-Performed informally (ad-hoc); 2-Partially implemented; 3-Close to completion; 4-Fully implemented; 5-Continuously improving (optimized) by ticking <i>V</i> one check box per question.							
i.	Does your institution have an information security policy that has been approved by top management?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ii.	Does the institution information security policy has been published and communicated to all relevant parties?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iii.	Does your institution review the information security policy at defined intervals to encompass significant change and monitor for compliance?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
iv.	Does your organization perform screening/ background checks (vetting) of employees?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
v.	Does your institution conduct security awareness, training and education?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vi.	Does your institution have an access control policy?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
vii.	Does your institution have encryption (cryptography) policy implemented?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
viii.	Does your institution have physical and environmental security policy developed and implemented?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
ix.	Does your institution have change management policy and acceptable use policy for information resources?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
x.	Does your institution have a network security policy implemented?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xi.	Does your institution have acquisition, development and maintenance policy implemented?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xii.	Does your institution have policies, procedures for managing supplier(s) relationships?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xiii.	Are standard operating procedures periodically evaluated for compliance with your organization's security policies, standards, and procedures?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xiv.	Does your institution perform periodic application and network layer vulnerability testing or penetration testing against critical IS?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>
xv.	Does your institution have a risk register and, it is regularly reviewed and updated?	0 <input type="checkbox"/>	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>	4 <input type="checkbox"/>	5 <input type="checkbox"/>

5. Comments and Suggestions (if any)

--

Thank you very much for your responses

B.5: Interview Data Collection Matrix Tool

(Chief Information Officer, Chief Information Security Officer or Equivalent, or a Designee)

Name of the organisation:

Part I: Security Requirements Assessment

FHEISCtool.xlsm data collection electronic tool was to be used

Part II: E-Services and Threat Analysis

1. What are the core e-services of the organization/department?

S/N	Name of e-services	Security Measures Available (VPN, https, ftps, secure login, secure financial transactions, SSH, smartcard, etc.)
1	1	

2. List challenges encountered and information security incidents occurred in your organization in the last 5 years to date

S/N	Challenges/ Incidents	Implications
1		
2		
3		
4		
5		

3. What is the percentage of the total budget allocated for information security?

Answer:

4. What do you think might be improved to increase the information system(s) security in your organization?

Answer:

5. What is the total number of IT staff in your organization?

Answer:

6. What is the total number of ICT Security staff in your organization?

Answer:

7. What is the total number of employees in your organization?

Answer:

8. What is the total number of Computers which are active in your network?

Answer:

9. How many subnets& VLAN current configured in LANs for your organization?

Answer:

Thank you very much for your responses

Appendix C: Data Analysis Tool for Capturing Responses

C.1: Logical Schema for Capturing Collected Data

FigureC.5 represents a logical diagram for the database used for capturing data collected after coding and used for data analysis.

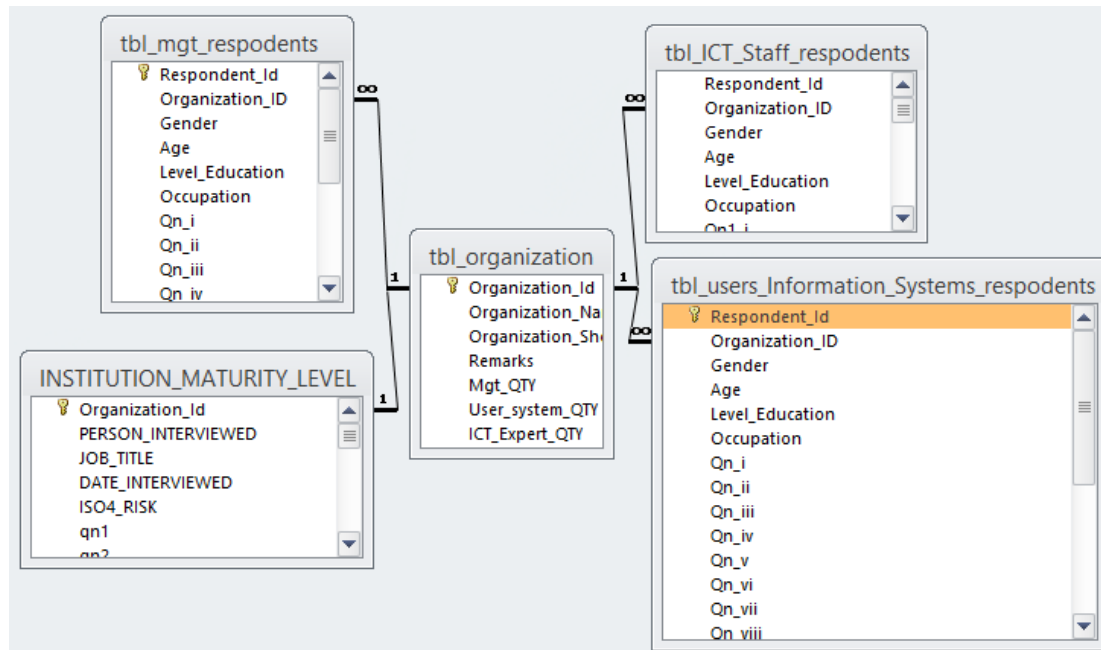


Figure C.1: Logical schema for data capturing tool

Table C.1: Education level profile for ICT Staff

Participant Education Level	Frequency	Percent
Postgraduate: MSc. Computer Science, Post graduate Diploma in IT	15	38.5
First Degree: Computer/IT	18	46.2
Advanced Diploma: IT	3	7.7
Ordinary Diploma: IT	2	5.1
PhD Student	1	2.6
Total	39	100.0

Appendix D: Source code for algorithm for enhanced security of information systems using cryptographic techniques

D.1: Source code for class EnhancedSecurityTransmissionCryptoTechniques

```
package ValidationofDevelopedFrameworkforEnhancingSecurityInformationSystems;
```

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.MessageDigest;
import java.security.PrivateKey;
import java.security.Signature;
import java.util.Scanner;

/**
 * @author mmshangi
 */
public class EnhancedSecurityTransmissionCryptoTechniques {

    public static void main(String args[]) throws Exception {
        //Methods for enhancing security using cryptographic techniques
        //Getting message i inputtext fro userx
        Scanner sc1 = new Scanner(System.in);
        System.out.println("Plaintext: please enter value for field i:");
        String msg1 = sc1.nextLine();
        System.out.println("");

        //Create te keys pair Generator object
        KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DSA");

        //Initialize the keys pair generator Object
        keyPairGen.initialize(2048);
        //Generate the pair of keys
        KeyPair pair = keyPairGen.generateKeyPair();
        //Getting the privatekey from the key pair
        PrivateKey privateKey = pair.getPrivate();

        //Begin creating Hash value
        //Creating the Hash value object
        MessageDigest hashValue = MessageDigest.getInstance("SHA-256");
        //Passing data to the created MessageDigest Object
        hashValue.update(msg1.getBytes());
        //Computing the hash value
        byte[] digest1 = hashValue.digest();
        //System.out.println(digest1);
        //Convert the byte array value in to Hexa decimal String value format
        StringBuffer hexString1 = new StringBuffer();
        for (int k = 0;k<digest1.length;k++) {
```

```

        hexString1.append(Integer.toHexString(0xFF & digest1[k]));
    }
    System.out.println("Message Digest: Hash value in Hex format : " +
        hexString1.toString());
    System.out.println("");
    //End creating Hash value

    //Creating a Signature object
    Signature sign1 = Signature.getInstance("SHA256withDSA");
    //Initializing the signature
    sign1.initSign(privateKey);
    byte[] bytes = hexString1.toString().getBytes();
    //Adding data to the signature
    sign1.update(bytes);
    //Computing the signature
    byte[] signature1 = sign1.sign();
    //Initializing the signature
    sign1.initVerify(pair.getPublic());
    sign1.update(bytes);
    System.out.println("Digital signature for given text: "+
        new String(signature1, "UTF8"));
    System.out.println("");

    //Verifying the signature
    boolean bool = sign1.verify(signature1);
    if(bool) {
        System.out.println("Signature verified is from the original source of message");
        System.out.println("");
        System.out.println("Public Key used to decrypt/verify signature:" +
            pair.getPublic());

    } else {
        System.out.println("Digital signature is invalid");
    }
}
}

```

D.2: Source code class EnhancedStorageSecurityCryptoTechniques

```
package ValidationofDevelopedFrameworkforEnhancingSecurityInformationSystems;
```

```
import java.sql.CallableStatement;
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.SQLException;

//@author mmshangi
public class EnhancedStorageSecurityCryptoTechniques {

    public static void main(String[] args)
    {
        //methods: Enhance security during storage at files level in database
        CallableStatement cstatement ;
        ResultSet recordSet ;
        try {
            Class.forName("com.microsoft.sqlserver.jdbc.SQLServerDriver");
            String connectionUrl = "jdbc:sqlserver://localhost:1433;" +
                "databaseName=StudentDb;user=xxxxx;password=yyyyyyy;";
            Connection con = DriverManager.getConnection(connectionUrl);

            cstatement = con.prepareCall(
                "{call proEncryptDecrypt}");
            cstatement.execute();
            recordSet = cstatement.getResultSet();
            while (recordSet.next())
            {
                int StudentId = recordSet.getInt("StudentId");
                String EncryptedStudentPhone =recordSet.getString("EncryptedStudentPhone");
                String DecryptedStudentPhone =recordSet.getString("DecryptedStudentPhone");
                String encryptedmarks =recordSet.getString("encryptedmarks");
                String DecryptedStudentMarks =recordSet.getString("DecryptedMarks");
                System.out.println(StudentId + "\t" + EncryptedStudentPhone + "\t" +
                    DecryptedStudentPhone + "\t" +encryptedmarks + "\t"
                    +DecryptedStudentMarks + "\t");
            }
        } catch (SQLException e1) {
            System.out.println("SQL Exception statement: " + e1.toString());
        } catch (ClassNotFoundException cE1) {
            System.out.println("No class Exception was found : " + cE1.toString());
        }
    }
}
```

Appendix E: Validation of the developed framework using Cryptographic techniques

E.1: Template for recording results of simulation experiment for algorithm for enhanced security of information systems using cryptographic techniques


Table E.1: Key size and execution time of the developed algorithm

Key size bits	Execution Time(ms)	
	DSA & SHA256	RSA & SHA256

E.2: Database schema for simulating enhancing security in information systems

Table E.2: Students information schema sample

.Stu... dbo.StudentInfo

Column Name	Data Type
 StudentId	int
StudentName	varchar(100)
StudentPhone	char(10)
SubjectCode	char(8)
Marks	numeric(18, 0)
EncryptedStudentPhone	varbinary(MAX)
EncryptedMarks	varbinary(MAX)

Appendix F: Published Papers

Paper I: The rapid growth of cybercrimes affecting information systems in the global: is a myth or reality in Tanzania

The main objective of this study was to determine whether the rapid growth of cybercrimes affecting information systems in the global: is a myth or reality in Tanzania. This paper was carried out to ascertain the status quo of security in the education sector in Tanzania, and it assisted in ascertaining the research problem and research gap. The paper was published in an international journal as detailed in the following paragraph.

Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). The Rapid Growth of Cybercrimes Affecting IS in the Global : Is this a Myth or Reality in Tanzania ? *International Journal of Information Security Science*, 3(2), 1826199.

http://ijiss.org/ijiss/index.php/ijiss/article/download/72/pdf_16

Paper II: Assessing security vulnerabilities in information systems, a case study of the education sector in Tanzania

This paper addressed RQ₂: “To what extents are the existing security controls ensure the security of information in information systems?” It assessed the implementation of the existing security controls in information systems during capturing, storage, processing and transmission in the education sector in Tanzania; using a case study of Heartbleed attack by carrying experiments using exploit Security tools (Filippo Heart-bleed test tool, Last Pass, Heartbleed checker, Qualys SSL Labs). The paper was published in the international journal under the title “Using Soft Systems Methodology and Activity Theory to Exploit Security of Web Applications against Heartbleed Vulnerability”. The details of the paper can be found as detailed in the following paragraph.

Mshangi, M., Nfuka, E. N., & Sanga, C. (2015). Using Soft Systems Methodology and Activity Theory to Exploit Security of Web Applications against Heartbleed Vulnerability. *International Journal of Computing and ICT Research*, 8(2), 32652. <http://ijcir.mak.ac.ug/volume8-number2/article4.pdf>

Paper III: Designing of secure information systems s architecture for the dissemination of information

The aim of this paper was to design secure information systems architecture for the dissemination of information in information systems in cyberspace. This addressed the research question, RQ₃: "How to develop a framework for enhancing the security of information systems?" This paper builds a foundation for developing a framework for enhancing security of information system; by designing design secure information systems architecture for information systems in cyberspace. The details of the paper published in the international journal are as follows.

Mshangi, M., Nfuka, E. N., & Sanga, C. (2016). Designing Secure Web and Mobile-Based Information System for Dissemination of Students ø Examination Results : The Suitability of Soft Design Science Methodology. *International Journal of Computing and ICT Research*, 10(2), 10640.<http://ijcir.mak.ac.ug/volume10-issue2/article2.pdf>

PaperIV: Framework for enhancing information systems security

The aim of the paper was to address the research question, RQ₃: "How to develop a framework for enhancing the security of information systems?". This was addressed by developing a framework for enhancing information systems security during information states. The developed framework for enhancing information systems security was published in the international journal under the title "An Innovative Soft Design Science Methodology for Improving Development of a Secure Information System in Tanzania Using Multi-Layered Approach." The detail of the can be found as specified in the following paragraph.

Mshangi, M., Nfuka, E. N., & Sanga, C. (2017). An Innovative Soft Design Science Methodology for Improving Development of a Secure Information System in Tanzania Using Multi-Layered Approach. *Journal of Information Security*, 8(3), 1416165.
<https://www.scirp.org/journal/PaperInformation.aspx?PaperID=77444>

Paper V: Human Sensor Web Crowd Sourcing Security Incidents Management in Tanzania Context

The aim of the paper was to address the research question, RQ₄: "How to validate the developed framework for enhancing the security of information systems". The study developed a prototype to simulate the real world implementation of the developed framework for enhancing the security of information systems. The paper proposes a human sensor web crowdsourcing platform for reporting, searching, querying, analysing, visualizing and responding to security incidents as they arise in real time. This paper was published in the international journal under the title "Human Sensor Web Crowdsourcing Security Incidents Management Platform". The detail of the can be found as specified in the following paragraph.

Mshangi, M., Nfuka, E. N., & Sanga, C. (2018). Human Sensor Web Crowdsourcing Security Incidents Management Platform. *Journal of Information Security*, 9(3), 1916208. <http://doi.org/10.4236/jis.2018.93014>